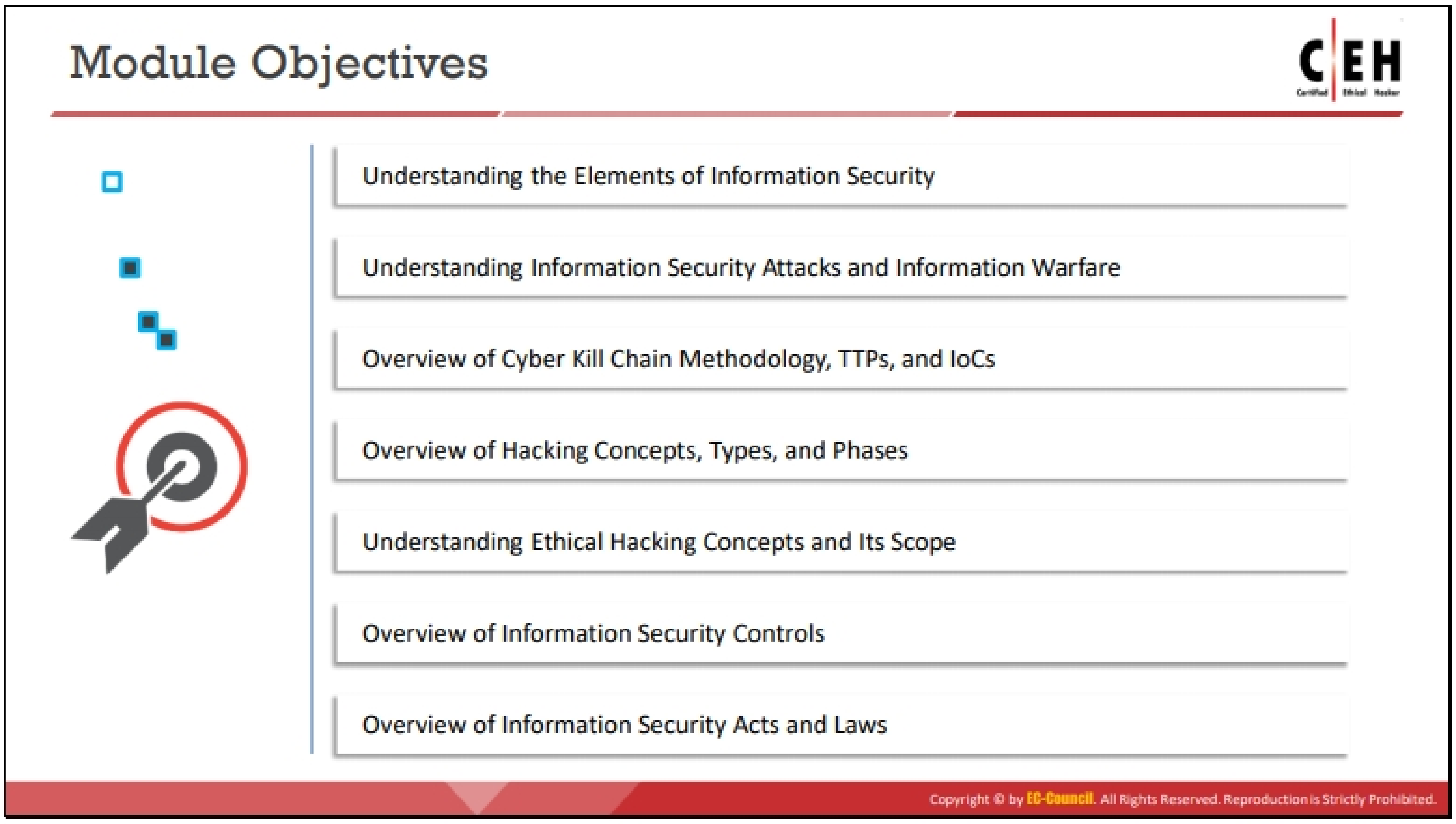
ETHICAL HACKING
THICAL
HACKIN
HACKING

C|EH™
Certified Ethical Hacker

Module 01:
Introduction to Ethical Hacking



Module Objectives

- Understanding the Elements of Information Security
- Understanding Information Security Attacks and Information Warfare
- Overview of Cyber Kill Chain Methodology, TTPs, and IoCs
- Overview of Hacking Concepts, Types, and Phases
- Understanding Ethical Hacking Concepts and Its Scope
- Overview of Information Security Controls
- Overview of Information Security Acts and Laws

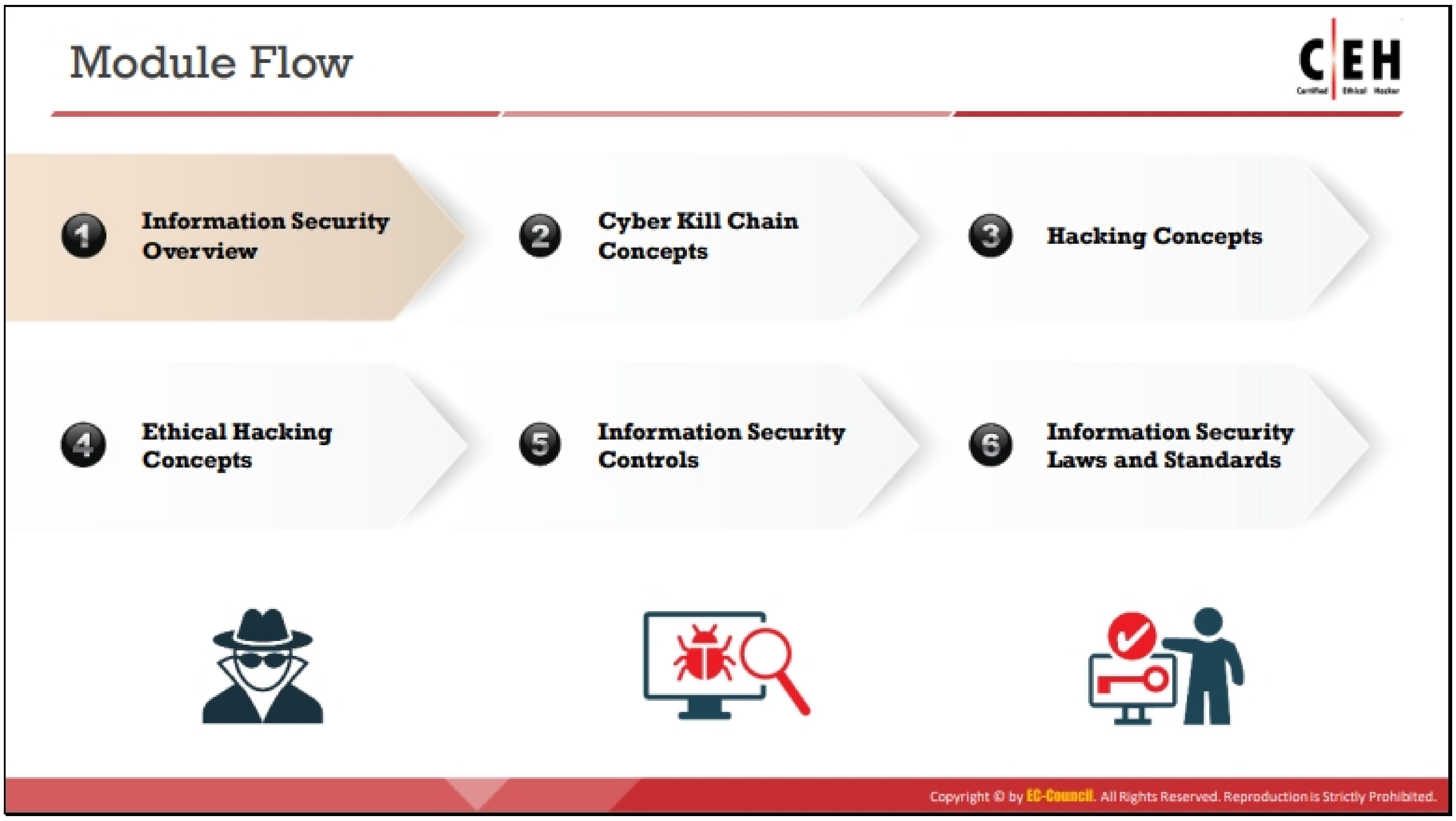
Module Objectives

Attackers break into systems for various reasons and purposes. Therefore, it is important to understand how malicious hackers attack and exploit systems and the probable reasons behind those attacks. As Sun Tzu states in the Art of War, “If you know yourself but not the enemy, for every victory gained, you will also suffer a defeat.” System administrators and security professionals must guard their infrastructure against exploits by knowing the enemy—the malicious hacker(s)—who seeks to use the same infrastructure for illegal activities.

This module starts with an overview of the current security scenario and emerging threat vectors. It provides insight into the different elements of information security. Later, the module discusses hacking and ethical hacking concepts and ends with a brief discussion on information security controls and information security laws and acts.

At the end of this module, you will be able to:

- Describe the elements of information security
- Explain information security attacks and information warfare
- Describe cyber kill chain methodology, TTPs, and IoCs
- Describe hacking concepts, types, and phases
- Explain ethical hacking concepts and scope
- Understand information security controls (defense-in-depth, risk management, cyber threat intelligence, threat modeling, incident management process, and AI/ML)
- Know about the information security acts and laws



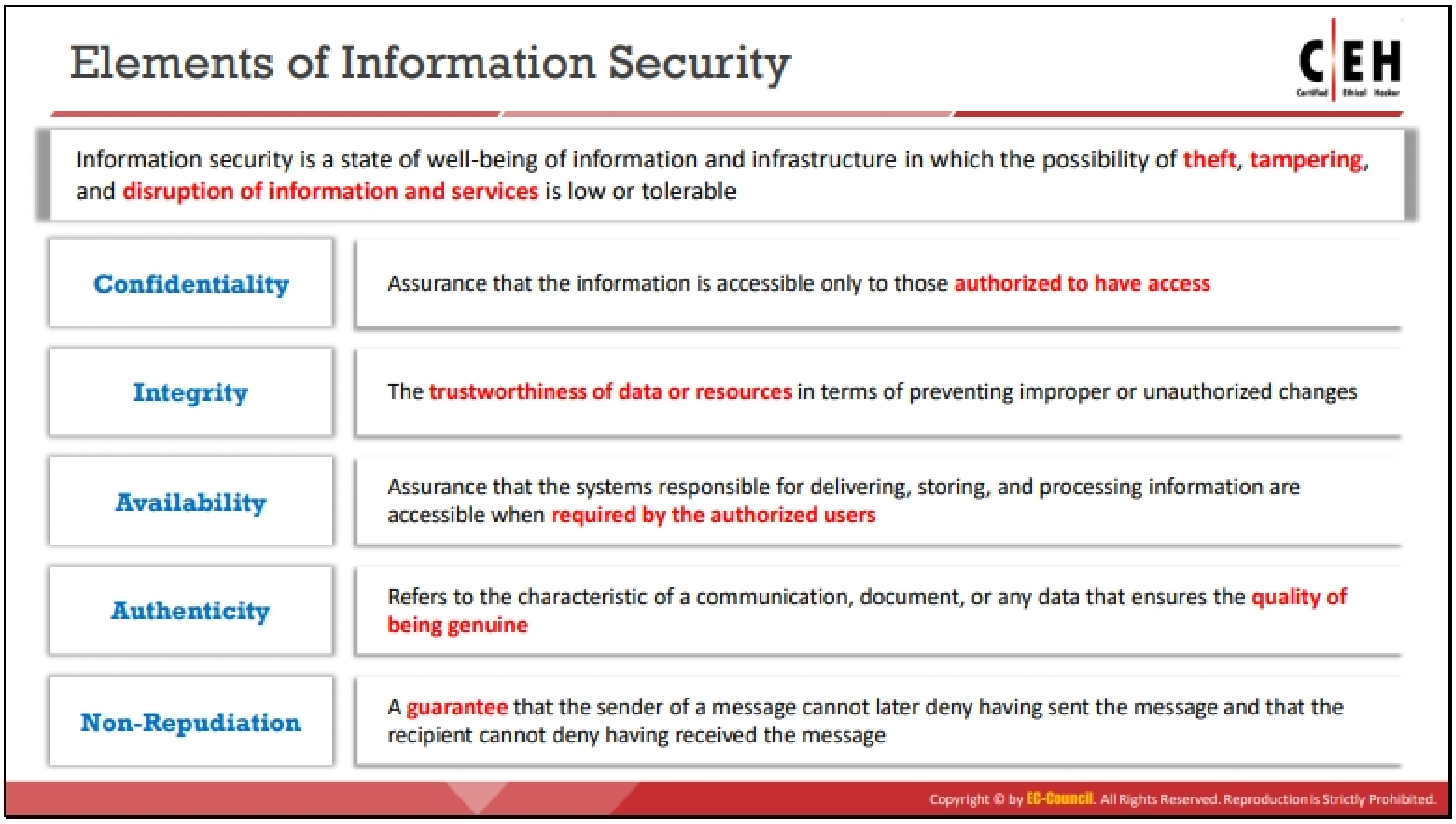
Module Flow

1. **Information Security Overview**
2. **Cyber Kill Chain Concepts**
3. **Hacking Concepts**
4. **Ethical Hacking Concepts**
5. **Information Security Controls**
6. **Information Security Laws and Standards**

Information Security Overview

Information security refers to the protection or safeguarding of information and information systems that use, store, and transmit information from unauthorized access, disclosure, alteration, and destruction. Information is a critical asset that organizations must secure. If sensitive information falls into the wrong hands, then the respective organization may suffer huge losses in terms of finances, brand reputation, customers, or in other ways. To provide an understanding of how to secure such critical information resources, this module starts with an overview of information security.

This section introduces the elements of information security, classification of attacks, and information warfare.



Elements of Information Security

Information security is a state of well-being of information and infrastructure in which the possibility of **theft**, **tampering**, and **disruption of information and services** is low or tolerable

Confidentiality	Assurance that the information is accessible only to those **authorized to have access**
Integrity	The **trustworthiness of data or resources** in terms of preventing improper or unauthorized changes
Availability	Assurance that the systems responsible for delivering, storing, and processing information are accessible when **required by the authorized users**
Authenticity	Refers to the characteristic of a communication, document, or any data that ensures the **quality of being genuine**
Non-Repudiation	A **guarantee** that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message

Elements of Information Security

Information security is "the state of the well-being of information and infrastructure in which the possibility of theft, tampering, or disruption of information and services is kept low or tolerable." It relies on five major elements: confidentiality, integrity, availability, authenticity, and non-repudiation.

- **Confidentiality**

  Confidentiality is the assurance that the information is accessible only to authorized. Confidentiality breaches may occur due to improper data handling or a hacking attempt. Confidentiality controls include data classification, data encryption, and proper disposal of equipment (such as DVDs, USB drives, and Blu-ray discs).

- **Integrity**

  Integrity is the trustworthiness of data or resources in the prevention of improper and unauthorized changes—the assurance that information is sufficiently accurate for its purpose. Measures to maintain data integrity may include a checksum (a number produced by a mathematical function to verify that a given block of data is not changed) and access control (which ensures that only authorized people can update, add, or delete data).

- **Availability**

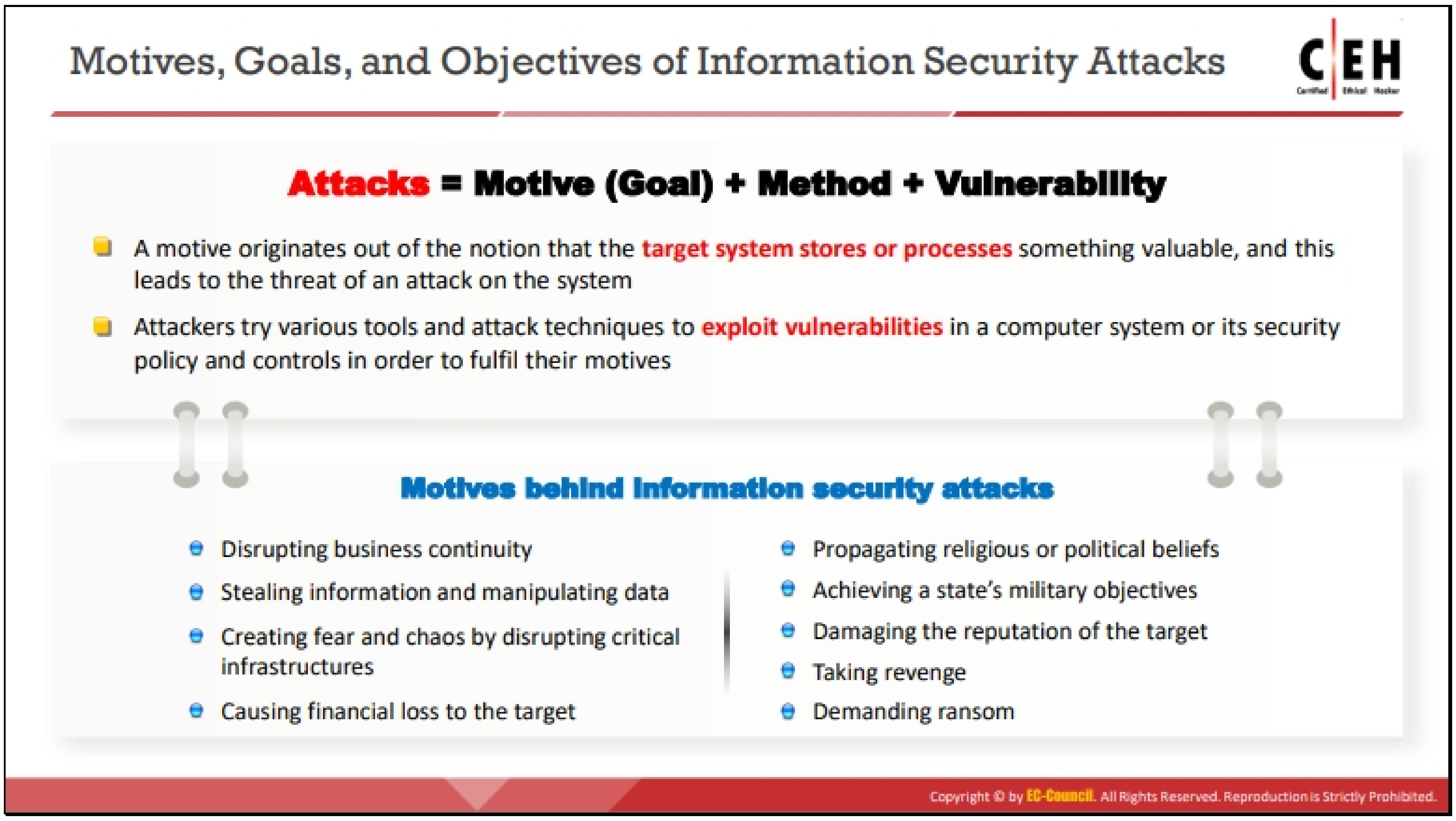
  Availability is the assurance that the systems responsible for delivering, storing, and processing information are accessible when required by authorized users. Measures to maintain data availability can include disk arrays for redundant systems and clustered machines, antivirus software to combat malware, and distributed denial-of-service (DDoS) prevention systems.

- **Authenticity**

  Authenticity refers to the characteristic of communication, documents, or any data that ensures the quality of being genuine or uncorrupted. The major role of authentication is to confirm that a user is genuine. Controls such as biometrics, smart cards, and digital certificates ensure the authenticity of data, transactions, communications, and documents.

- **Non-Repudiation**

  Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message. Individuals and organizations use digital signatures to ensure non-repudiation.



Motives, Goals, and Objectives of Information Security Attacks

Attacks = Motive (Goal) + Method + Vulnerability

- A motive originates out of the notion that the **target system stores or processes** something valuable, and this leads to the threat of an attack on the system
- Attackers try various tools and attack techniques to **exploit vulnerabilities** in a computer system or its security policy and controls in order to fulfil their motives

Motives behind information security attacks

- Disrupting business continuity
- Stealing information and manipulating data
- Creating fear and chaos by disrupting critical infrastructures
- Causing financial loss to the target
- Propagating religious or political beliefs
- Achieving a state's military objectives
- Damaging the reputation of the target
- Taking revenge
- Demanding ransom

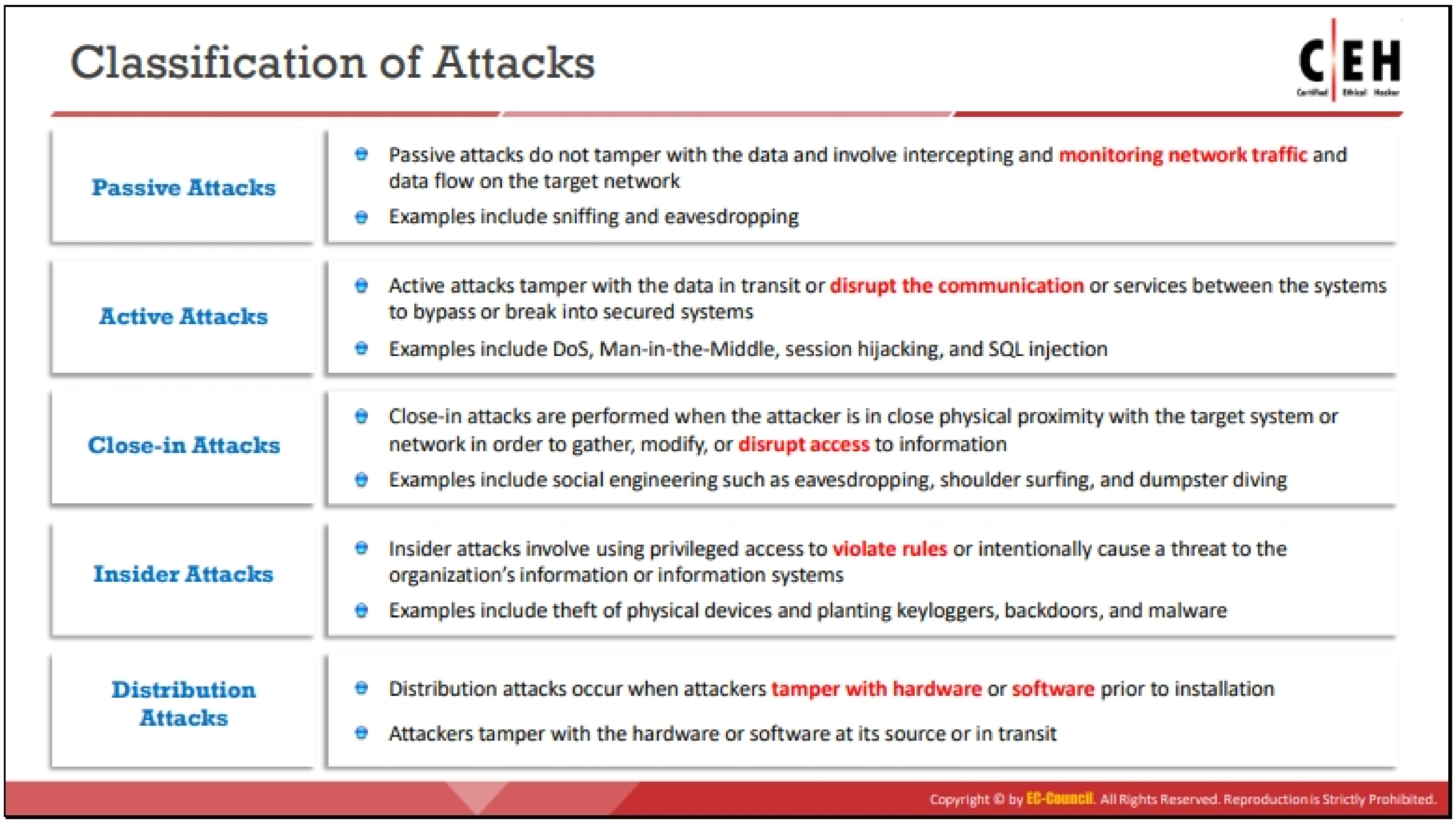
Motives, Goals, and Objectives of Information Security Attacks

Attackers generally have motives (goals), and objectives behind their information security attacks. A motive originates out of the notion that a target system stores or processes something valuable, which leads to the threat of an attack on the system. The purpose of the attack may be to disrupt the target organization's business operations, to steal valuable information for the sake of curiosity, or even to exact revenge. Therefore, these motives or goals depend on the attacker's state of mind, their reason for carrying out such an activity, as well as their resources and capabilities. Once the attacker determines their goal, they can employ various tools, attack techniques, and methods to exploit vulnerabilities in a computer system or security policy and controls.

Attacks = Motive (Goal) + Method + Vulnerability

Motives behind information security attacks

- Disrupt business continuity
- Perform information theft
- Manipulating data
- Create fear and chaos by disrupting critical infrastructures
- Bring financial loss to the target
- Propagate religious or political beliefs
- Achieve a state's military objectives
- Damage the reputation of the target
- Take revenge
- Demand ransom



Classification of Attacks

Passive Attacks	Passive attacks do not tamper with the data and involve intercepting and **monitoring network traffic** and data flow on the target network Examples include sniffing and eavesdropping
Active Attacks	Active attacks tamper with the data in transit or **disrupt the communication** or services between the systems to bypass or break into secured systems Examples include DoS, Man-in-the-Middle, session hijacking, and SQL injection
Close-in Attacks	Close-in attacks are performed when the attacker is in close physical proximity with the target system or network in order to gather, modify, or **disrupt access** to information Examples include social engineering such as eavesdropping, shoulder surfing, and dumpster diving
Insider Attacks	Insider attacks involve using privileged access to **violate rules** or intentionally cause a threat to the organization's information or information systems Examples include theft of physical devices and planting keyloggers, backdoors, and malware
Distribution Attacks	Distribution attacks occur when attackers **tamper with hardware** or **software** prior to installation Attackers tamper with the hardware or software at its source or in transit

Classification of Attacks

According to IATF, security attacks are classified into five categories: passive, active, close-in, insider, and distribution.

- **Passive Attacks**

  Passive attacks involve intercepting and monitoring network traffic and data flow on the target network and do not tamper with the data. Attackers perform reconnaissance on network activities using sniffers. These attacks are very difficult to detect as the attacker has no active interaction with the target system or network. Passive attacks allow attackers to capture the data or files being transmitted in the network without the consent of the user. For example, an attacker can obtain information such as unencrypted data in transit, clear-text credentials, or other sensitive information that is useful in performing active attacks.

  Examples of passive attacks:

  - Footprinting
  - Sniffing and eavesdropping
  - Network traffic analysis
  - Decryption of weakly encrypted traffic

- **Active Attacks**

  Active attacks tamper with the data in transit or disrupt communication or services between the systems to bypass or break into secured systems. Attackers launch attacks on the target system or network by sending traffic actively that can be detected. These attacks are performed on the target network to exploit the information in transit. They penetrate or infect the target's internal network and gain access to a remote system to compromise the internal network.

Examples of active attacks:

- Denial-of-service (DoS) attack
- Bypassing protection mechanisms
- Malware attacks (such as viruses, worms, ransomware)
- Modification of information
- Spoofing attacks
- Replay attacks
- Password-based attacks
- Session hijacking
- Man-in-the-Middle attack
- DNS and ARP poisoning
- Compromised-key attack
- Firewall and IDS attack
- Profiling
- Arbitrary code execution
- Privilege escalation
- Backdoor access
- Cryptography attacks
- SQL injection
- XSS attacks
- Directory traversal attacks
- Exploitation of application and OS software

- **Close-in Attacks**

  Close-in attacks are performed when the attacker is in close physical proximity with the target system or network. The main goal of performing this type of attack is to gather or modify information or disrupt its access. For example, an attacker might shoulder surf user credentials. Attackers gain close proximity through surreptitious entry, open access, or both.

  Examples of close-in attacks:

  - Social engineering (Eavesdropping, shoulder surfing, dumpster diving, and other methods)

- **Insider Attacks**

  Insider attacks are performed by trusted persons who have physical access to the critical assets of the target. An insider attack involves using privileged access to violate rules or intentionally cause a threat to the organization's information or information systems. Insiders can easily bypass security rules, corrupt valuable resources, and access sensitive information. They misuse the organization's assets to directly affect the confidentiality, integrity, and availability of information systems. These attacks impact the organization's business operations, reputation, and profit. It is difficult to figure out an insider attack

  Examples of insider attacks:

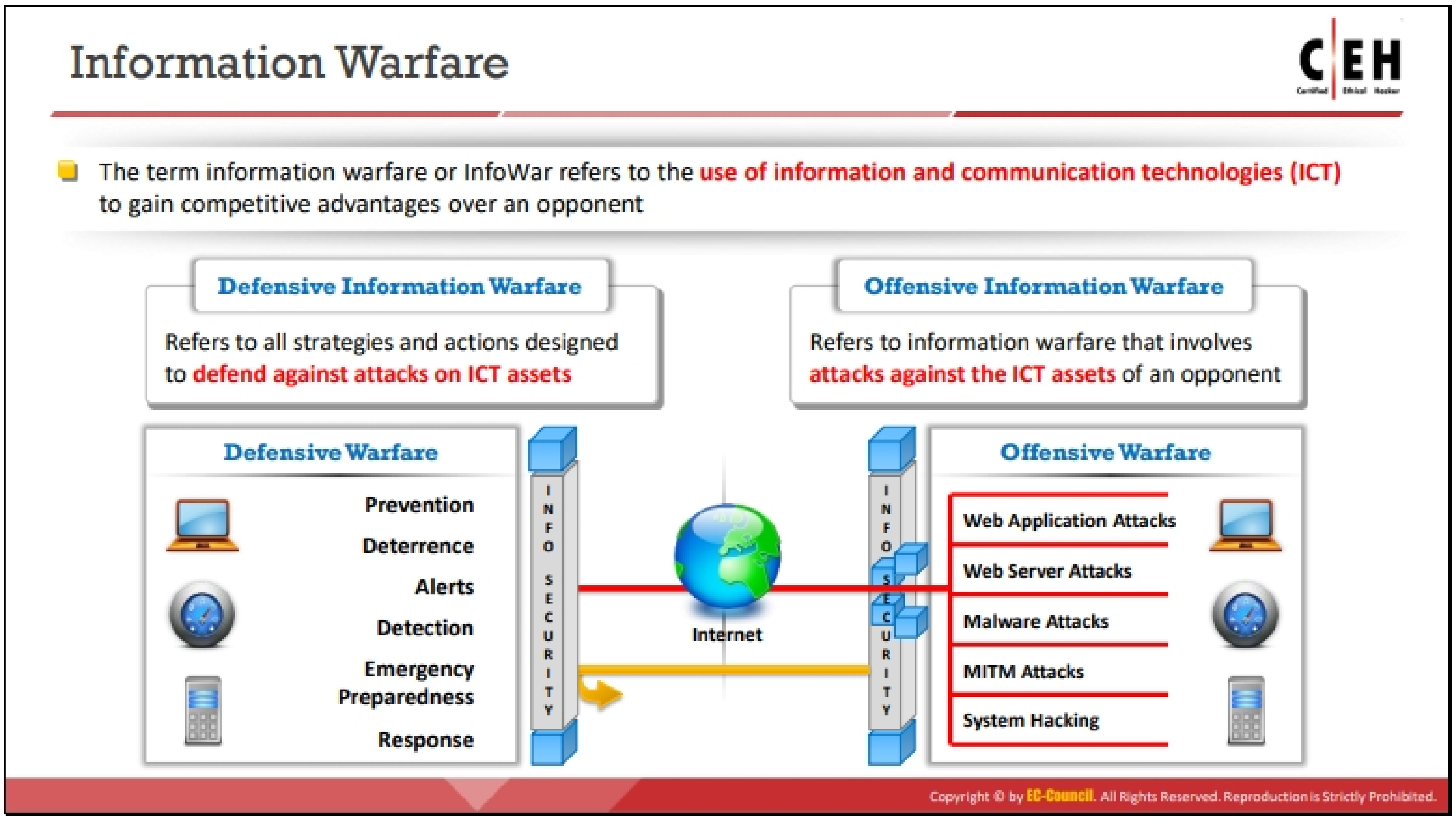
  - Eavesdropping and wiretapping

  - Theft of physical devices
  - Social engineering
  - Data theft and spoliation
  - Pod slurping
  - Planting keyloggers, backdoors, or malware

- **Distribution Attacks**

  Distribution attacks occur when attackers tamper with hardware or software prior to installation. Attackers tamper the hardware or software at its source or when it is in transit. Examples of distribution attacks include backdoors created by software or hardware vendors at the time of manufacture. Attackers leverage these backdoors to gain unauthorized access to the target information, systems, or network.

  - Modification of software or hardware during production
  - Modification of software or hardware during distribution



Information Warfare

- The term information warfare or InfoWar refers to the **use of information and communication technologies (ICT)** to gain competitive advantages over an opponent

Defensive Information Warfare

Refers to all strategies and actions designed to **defend against attacks on ICT assets**

Offensive Information Warfare

Refers to information warfare that involves **attacks against the ICT assets** of an opponent

Defensive Warfare

- Prevention
- Deterrence
- Alerts
- Detection
- Emergency Preparedness
- Response

Offensive Warfare

- Web Application Attacks
- Web Server Attacks
- Malware Attacks
- MITM Attacks
- System Hacking

Information Warfare

Source: *http://www.iwar.org.uk*

The term information warfare or InfoWar refers to the use of information and communication technologies (ICT) for competitive advantages over an opponent. Examples of information warfare weapons include viruses, worms, Trojan horses, logic bombs, trap doors, nanomachines and microbes, electronic jamming, and penetration exploits and tools.

Martin Libicki divided information warfare into the following categories:

- **Command and control warfare (C2 warfare)**: In the computer security industry, C2 warfare refers to the impact an attacker possesses over a compromised system or network that they control.
- **Intelligence-based warfare**: Intelligence-based warfare is a sensor-based technology that directly corrupts technological systems. According to Libicki, "intelligence-based warfare" is warfare that consists of the design, protection, and denial of systems that seek sufficient knowledge to dominate the battlespace.
- **Electronic warfare**: According to Libicki, electronic warfare uses radio-electronic and cryptographic techniques to degrade communication. Radio electronic techniques attack the physical means of sending information, whereas cryptographic techniques use bits and bytes to disrupt the means of sending information.
- **Psychological warfare**: Psychological warfare is the use of various techniques such as propaganda and terror to demoralize one's adversary in an attempt to succeed in battle.
- **Hacker warfare**: According to Libicki, the purpose of this type of warfare can vary from the shutdown of systems, data errors, theft of information, theft of services, system

monitoring, false messaging, and access to data. Hackers generally use viruses, logic bombs, Trojan horses, and sniffers to perform these attacks.

- **Economic warfare**: Libicki notes that economic information warfare can affect the economy of a business or nation by blocking the flow of information. This could be especially devastating to organizations that do a lot of business in the digital world.
- **Cyberwarfare**: Libicki defines cyber warfare as the use of information systems against the virtual personas of individuals or groups. It is the broadest of all information warfare. It includes information terrorism, semantic attacks (similar to Hacker warfare, but instead of harming a system, it takes over the system while maintaining the perception that it is operating correctly), and simula-warfare (simulated war, for example, acquiring weapons for mere demonstration rather than actual use).

Each form of information warfare mentioned above consists of both defensive and offensive strategies.

- **Defensive Information Warfare**: Involves all strategies and actions to defend against attacks on ICT assets.
- **Offensive Information Warfare**: Involves attacks against the ICT assets of an opponent.

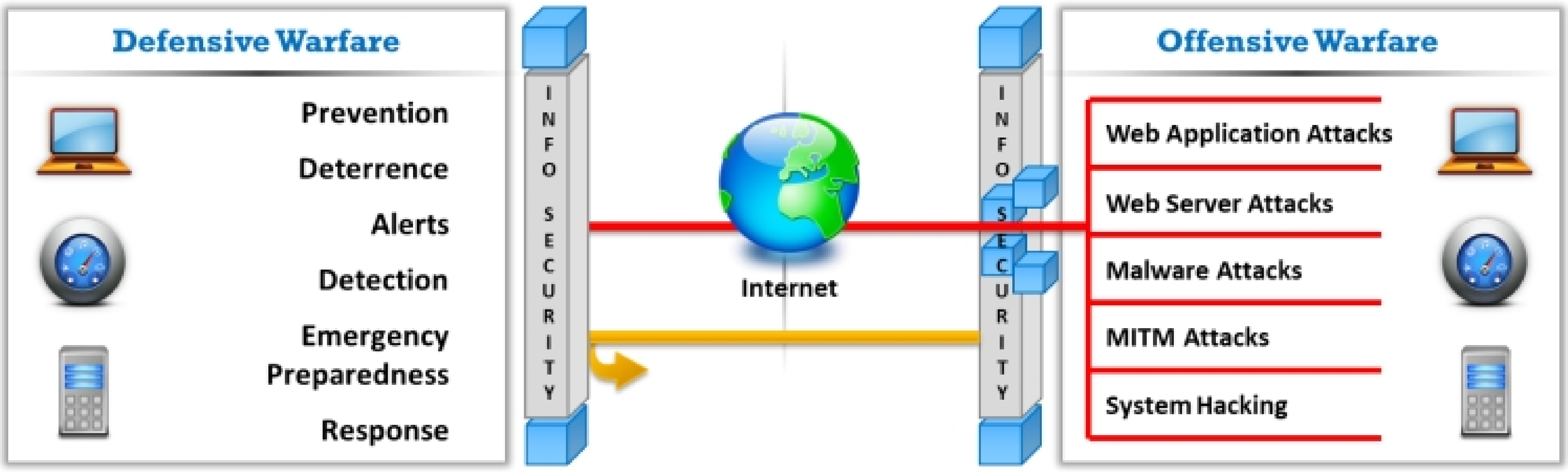
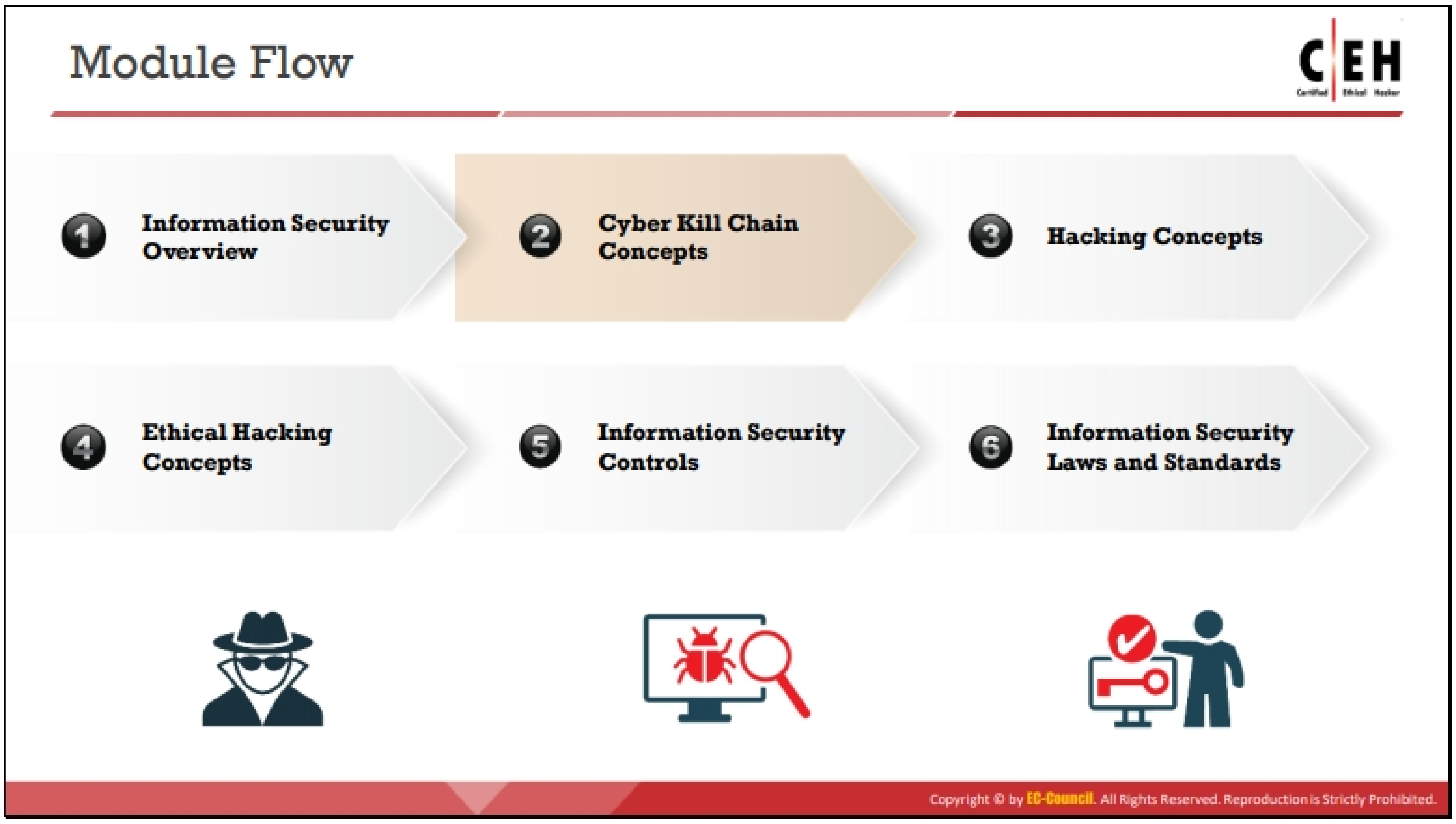

Defensive Warfare
Prevention
Deterrence
Alerts
Detection
Emergency Preparedness
Response
INFO SECURITY
Internet
INFO SECURITY
Offensive Warfare
Web Application Attacks
Web Server Attacks
Malware Attacks
MITM Attacks
System Hacking

Figure 1.1: Block Diagram of Information Warfare



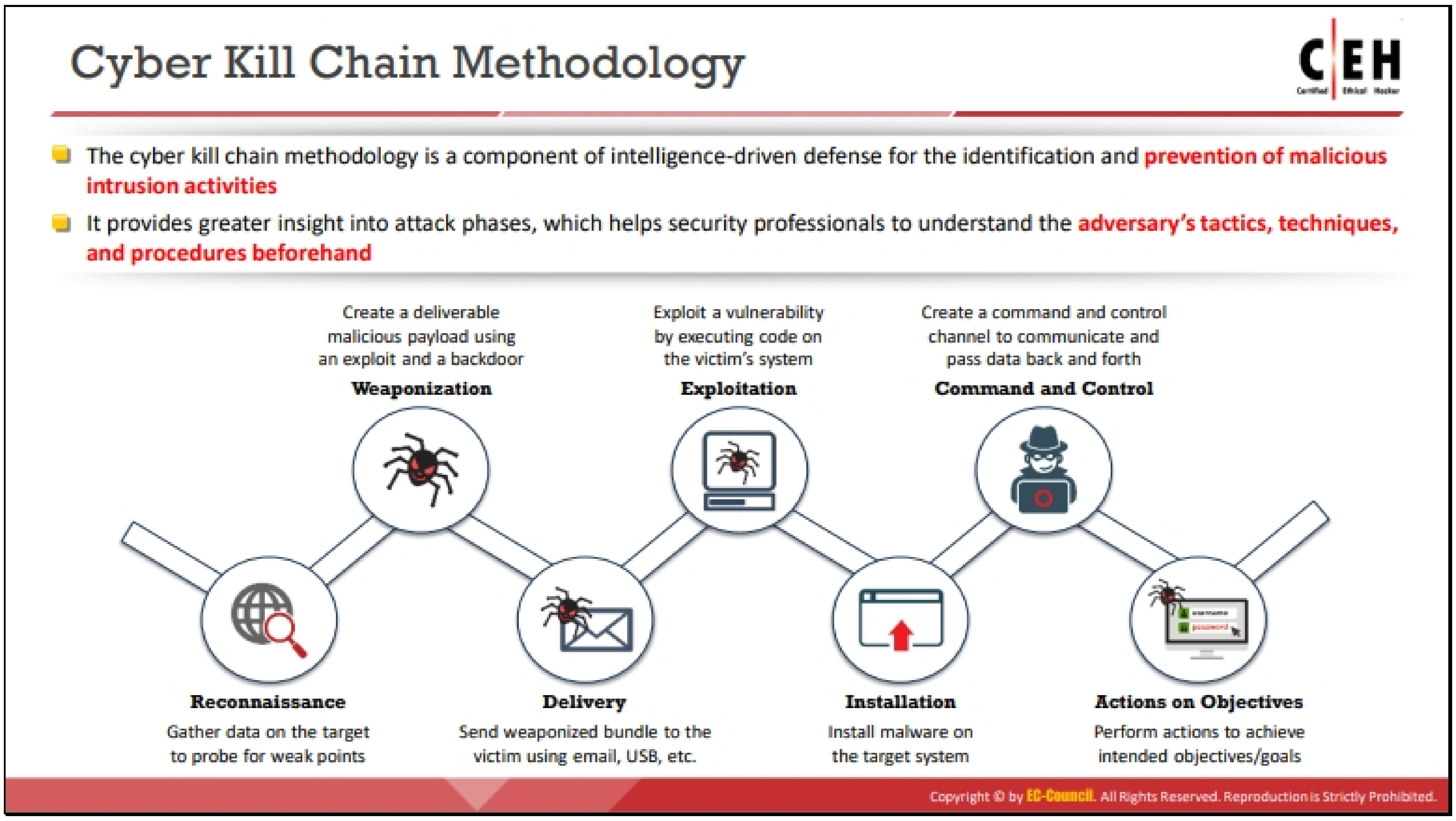
Module Flow

1. Information Security Overview
2. Cyber Kill Chain Concepts
3. Hacking Concepts
4. Ethical Hacking Concepts
5. Information Security Controls
6. Information Security Laws and Standards

Cyber Kill Chain Concepts

The cyber kill chain is an efficient and effective way of illustrating how an adversary can attack the target organization. This model helps organizations understand the various possible threats at every stage of an attack and the necessary countermeasures to defend against such attacks. Also, this model provides security professionals with a clear insight into the attack strategy used by the adversary so that different levels of security controls can be implemented to protect the IT infrastructure of the organization.

This section discusses the cyber kill chain methodology, common TTPs used by adversaries, behavioral identification of adversaries, and Indicators of Compromise (IoCs).



Cyber Kill Chain Methodology

- The cyber kill chain methodology is a component of intelligence-driven defense for the identification and **prevention of malicious intrusion activities**
- It provides greater insight into attack phases, which helps security professionals to understand the **adversary's tactics, techniques, and procedures beforehand**

Reconnaissance
Gather data on the target to probe for weak points

Weaponization
Create a deliverable malicious payload using an exploit and a backdoor

Delivery
Send weaponized bundle to the victim using email, USB, etc.

Exploitation
Exploit a vulnerability by executing code on the victim's system

Installation
Install malware on the target system

Command and Control
Create a command and control channel to communicate and pass data back and forth

Actions on Objectives
Perform actions to achieve intended objectives/goals

Cyber Kill Chain Methodology

The cyber kill chain methodology is a component of intelligence-driven defense for the identification and prevention of malicious intrusion activities. This methodology helps security professionals in identifying the steps that adversaries follow in order to accomplish their goals.

The cyber kill chain is a framework developed for securing cyberspace based on the concept of military kill chains. This method aims to actively enhance intrusion detection and response. The cyber kill chain is equipped with a seven-phase protection mechanism to mitigate and reduce cyber threats.

According to Lockheed Martin, cyberattacks might occur in seven different phases, from reconnaissance to the final accomplishment of the objective. An understanding of cyber kill chain methodology helps security professionals to leverage security controls at different stages of an attack and helps them to prevent the attack before it succeeds. It also provides greater insight into the attack phases, which helps in understanding the adversary's TTPs beforehand.

Discussed below are various phases included in cyber kill chain methodology:

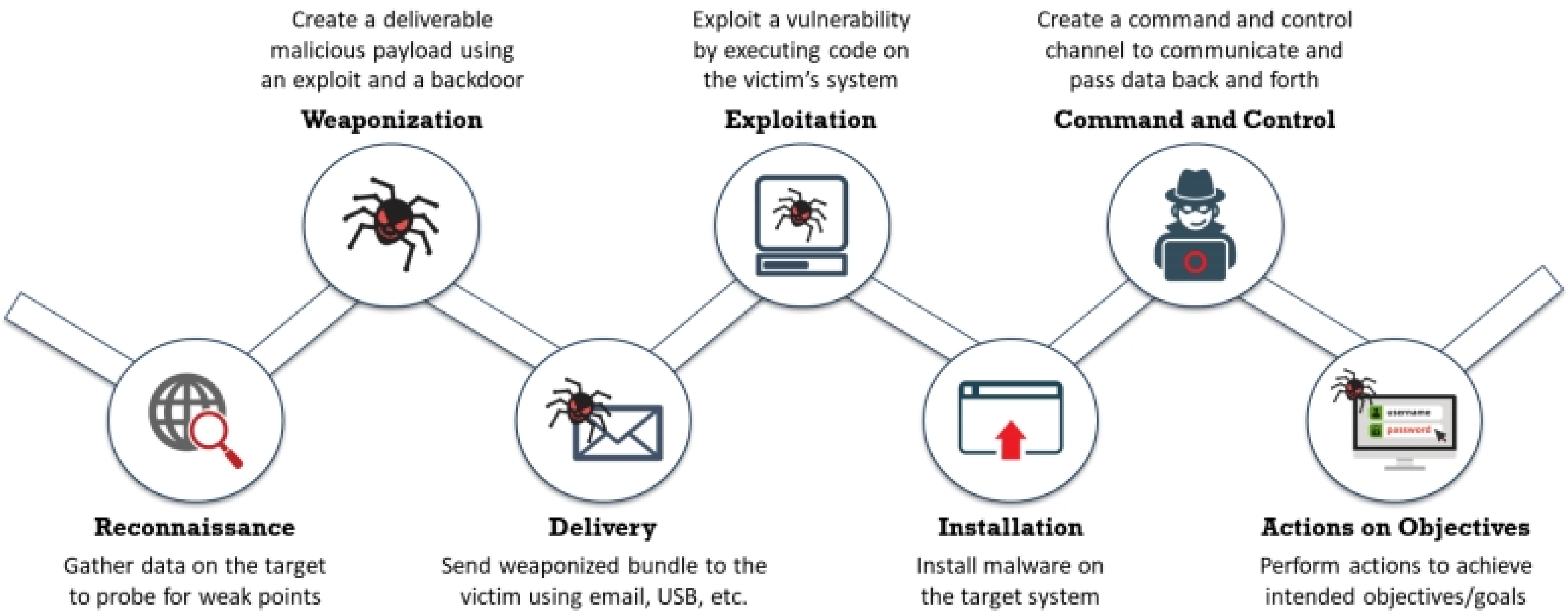

Create a deliverable malicious payload using an exploit and a backdoor
Weaponization
Exploit a vulnerability by executing code on the victim's system
Exploitation
Create a command and control channel to communicate and pass data back and forth
Command and Control
username
password
Reconnaissance
Gather data on the target to probe for weak points
Delivery
Send weaponized bundle to the victim using email, USB, etc.
Installation
Install malware on the target system
Actions on Objectives
Perform actions to achieve intended objectives/goals

Figure 1.2: Cyber kill chain methodology

- **Reconnaissance**

  An adversary performs reconnaissance to collect as much information about the target as possible to probe for weak points before actually attacking. They look for information such as publicly available information on the Internet, network information, system information, and the organizational information of the target. By conducting reconnaissance across different network levels, the adversary can gain information such as network blocks, specific IP addresses, and employee details. The adversary may use automated tools such as open ports and services, vulnerabilities in applications, and login credentials, to obtain information. Such information can help the adversary in gaining backdoor access to the target network.

  Activities of the adversary include the following:

  - Gathering information about the target organization by searching the Internet or through social engineering
  - Performing analysis of various online activities and publicly available information
  - Gathering information from social networking sites and web services
  - Obtaining information about websites visited
  - Monitoring and analyzing the target organization's website
  - Performing Whois, DNS, and network footprinting
  - Performing scanning to identify open ports and services

- **Weaponization**

  The adversary analyzes the data collected in the previous stage to identify the vulnerabilities and techniques that can exploit and gain unauthorized access to the target organization. Based on the vulnerabilities identified during analysis, the adversary selects or creates a tailored deliverable malicious payload (remote-access malware weapon) using an exploit and a backdoor to send it to the victim. An adversary may target specific network devices, operating systems, endpoint devices, or even individuals within the organization to carry out their attack. For example, the adversary may send a phishing email to an employee of the target organization, which may include a malicious attachment such as a virus or worm that, when downloaded, installs a backdoor on the system that allows remote access to the adversary.

The following are the activities of the adversary:

- Identifying appropriate malware payload based on the analysis
- Creating a new malware payload or selecting, reusing, modifying the available malware payloads based on the identified vulnerability
- Creating a phishing email campaign
- Leveraging exploit kits and botnets

- **Delivery**

  The previous stage included creating a weapon. Its payload is transmitted to the intended victim(s) as an email attachment, via a malicious link on websites, or through a vulnerable web application or USB drive. Delivery is a key stage that measures the effectiveness of the defense strategies implemented by the target organization based on whether the intrusion attempt of the adversary is blocked or not.

  The following are the activities of the adversary:

  - Sending phishing emails to employees of the target organization
  - Distributing USB drives containing malicious payload to employees of the target organization
  - Performing attacks such as watering hole on the compromised website
  - Implementing various hacking tools against the operating systems, applications, and servers of the target organization

- **Exploitation**

  After the weapon is transmitted to the intended victim, exploitation triggers the adversary's malicious code to exploit a vulnerability in the operating system, application, or server on a target system. At this stage, the organization may face threats such as authentication and authorization attacks, arbitrary code execution, physical security threats, and security misconfiguration.

  Activities of the adversary include the following:

  - Exploiting software or hardware vulnerabilities to gain remote access to the target system

- **Installation**

  The adversary downloads and installs more malicious software on the target system to maintain access to the target network for an extended period. They may use the weapon to install a backdoor to gain remote access. After the injection of the malicious code on one target system, the adversary gains the capability to spread the infection to other end systems in the network. Also, the adversary tries to hide the presence of malicious activities from security controls like firewalls using various techniques such as encryption.

  The following are the activities of the adversary:

  - Downloading and installing malicious software such as backdoors
  - Gaining remote access to the target system
  - Leveraging various methods to keep backdoor hidden and running
  - Maintaining access to the target system

- **Command and Control**

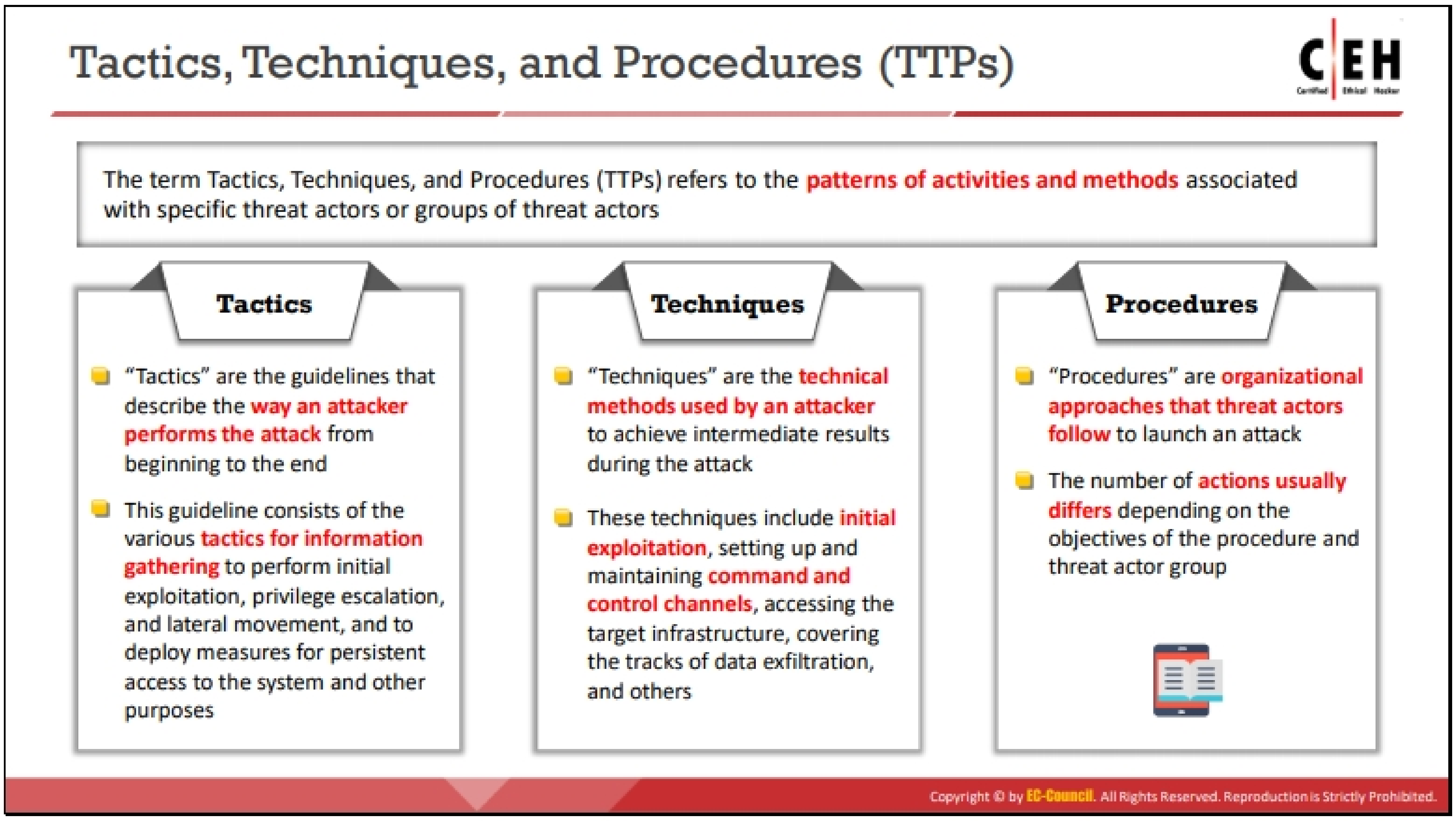
  The adversary creates a command and control channel, which establishes two-way communication between the victim's system and adversary-controlled server to communicate and pass data back and forth. The adversaries implement techniques such as encryption to hide the presence of such channels. Using this channel, the adversary performs remote exploitation on the target system or network.

  The following are the activities of the adversary:

  - Establishing a two-way communication channel between the victim's system and the adversary-controlled server
  - Leveraging channels such as web traffic, email communication, and DNS messages.
  - Applying privilege escalation techniques
  - Hiding any evidence of compromise using techniques such as encryption

- **Actions on Objectives**

  The adversary controls the victim's system from a remote location and finally accomplishes their intended goals. The adversary gains access to confidential data, disrupts the services or network, or destroys the operational capability of the target by gaining access to its network and compromising more systems. Also, the adversary may use this as a launching point to perform other attacks.



Tactics, Techniques, and Procedures (TTPs)

The term Tactics, Techniques, and Procedures (TTPs) refers to the **patterns of activities and methods** associated with specific threat actors or groups of threat actors

Tactics

- "Tactics" are the guidelines that describe the **way an attacker performs the attack** from beginning to the end
- This guideline consists of the various **tactics for information gathering** to perform initial exploitation, privilege escalation, and lateral movement, and to deploy measures for persistent access to the system and other purposes

Techniques

- "Techniques" are the **technical methods used by an attacker** to achieve intermediate results during the attack
- These techniques include **initial exploitation**, setting up and maintaining **command and control channels**, accessing the target infrastructure, covering the tracks of data exfiltration, and others

Procedures

- "Procedures" are **organizational approaches that threat actors follow** to launch an attack
- The number of **actions usually differs** depending on the objectives of the procedure and threat actor group

Tactics, Techniques, and Procedures (TTPs)

The terms "tactics, techniques, and procedures" refer to the patterns of activities and methods associated with specific threat actors or groups of threat actors. TTPs are helpful in analyzing threats and profiling threat actors and can further be used to strengthen the security infrastructure of an organization. The word "tactics" is defined as a guideline that describes the way an attacker performs their attack from beginning to end. The word "techniques" is defined as the technical methods used by an attacker to achieve intermediate results during their attack. Finally, the word "procedures" is defined as the organizational approach followed by the threat actors to launch their attack. In order to understand and defend against the threat actors, it is important to understand the TTPs used by adversaries. Understanding the tactics of an attacker helps to predict and detect evolving threats in the early stages. Understanding the techniques used by attackers helps to identify vulnerabilities and implement defensive measures in advance. Lastly, analyzing the procedures used by the attackers helps to identify what the attacker is looking for within the target organization's infrastructure.

Organizations should understand TTPs to protect their network against threat actors and upcoming attacks. TTPs enable the organizations to stop attacks at the initial stage, thereby protecting the network against massive damages.

- **Tactics**

  Tactics describe the way the threat actor operates during different phases of an attack. It consists of the various tactics used to gather information for the initial exploitation, perform privilege escalation and lateral movement, and deploy measures for persistence access to the system. Generally, APT groups depend on a certain set of unchanging tactics, but in some cases, they adapt to different circumstances and alter the way they perform their attacks. Therefore, the difficulty of detecting and attributing the attack campaign depends on the tactics used to perform the attack.

An organization can profile threat actors based on tactics they use; this consists of the way they gather information about a target, the methods they follow for initial compromise, and the number of entry points they use while attempting to enter the target network.

For example, to obtain information, some threat actors depend solely on information available on the Internet, whereas others might perform social engineering or use connections in intermediate organizations. Once information such as the email addresses of employees of the target organization is gathered, the threat actors either choose to approach the target one by one or as a group. Furthermore, the attackers' designed payload can stay constant from the beginning to the end of the attack or may be changed based on the targeted individual. Therefore, to understand the threat actors better, tactics used in the early stages of an attack must be analyzed properly.

Another method of analyzing the APT groups is inspecting the infrastructure and tools used to perform their attack. For example, consider establishing a command and control channel on the servers controlled by the attacker. These C&C servers may be located within a specific geographical location or may spread across the Internet and can be static or can change dynamically. It is also important to analyze the tools used to perform the attack. This includes analyzing the exploits and tools used by various APT groups. In such a scenario, a sophisticated threat actor may exploit many zero-day vulnerabilities by using adapted tools and obfuscation methods. However, this might be difficult as less-sophisticated threat actors generally depend on publicly known vulnerabilities and open-source tools. Identifying this type of tactic helps in profiling the APT groups and building defensive measures in advance.

In some cases, understanding the tactics used in the last stages of an attack helps in profiling the threat actor. Also, the methods used to cover the tracks help the target organization understand attack campaigns. Analyzing the tactics used by the attackers helps in creating an initial profile by understanding different phases of an APT life cycle. This profile helps in performing further analysis of the techniques and procedures used by the attackers. An attacker may continually change the TTPs used, so it is important to constantly review and update the tactics used by the APT groups.

- **Techniques**

  To launch an attack successfully, threat actors use several techniques during its execution. These techniques include initial exploitation, setting up and maintaining command and control channels, accessing the target infrastructure, and covering the tracks of data exfiltration. The techniques followed by the threat actor to conduct an attack might vary, but they are mostly similar and can be used for profiling. Therefore, understanding the techniques used in the different phases of an attack is essential to analyzing the threat groups effectively.

Techniques can also be analyzed at each stage of the threat life cycle. Therefore, the techniques at the initial stage mainly describe the tools used for information gathering and initial exploitation. The techniques used in this stage need not necessarily have a technical aspect. For example, in social engineering, certain non-technical software tools are used as an effective way of gathering information. An attacker can use such tools to obtain the email addresses of target organization employees through publicly available resources.

In the same manner, purely human-based social engineering can be used to perform the initial exploitation. For example, consider a scenario where the victim is tricked via a phone call to reveal their login credentials for accessing the target organization's internal network. These techniques are used in the initial phase of an attack to gather information about the target and break the first line of defense.

Techniques used in the middle stages of an attack mostly depend on technical tools for initially escalating privileges on systems that are compromised or performing lateral movements within the target organization's network. At this stage of an attack, the attackers use various exploits or misuse configuration vulnerabilities on the target system. They may also exploit network design flaws to gain access to other systems in the network. In all of these cases, either exploits or a collection of tools allows the attacker to perform a successful attack. In this scenario, the term "technique" is the set of tools and the way they are used to obtain intermediate results during an attack campaign.

The techniques in the last stage of an attack can have both technical and nontechnical aspects. In such a scenario, the techniques used for data-stealing are usually based on network technology and encryption. For example, the threat actor encrypts the stolen files, transfers them through the established command and control channel, and copies them to their own system. After successfully executing the attack and transferring the files, the attacker follows certain purely technical techniques to cover their tracks. They use automated software tools to clear logs files to evade detection.

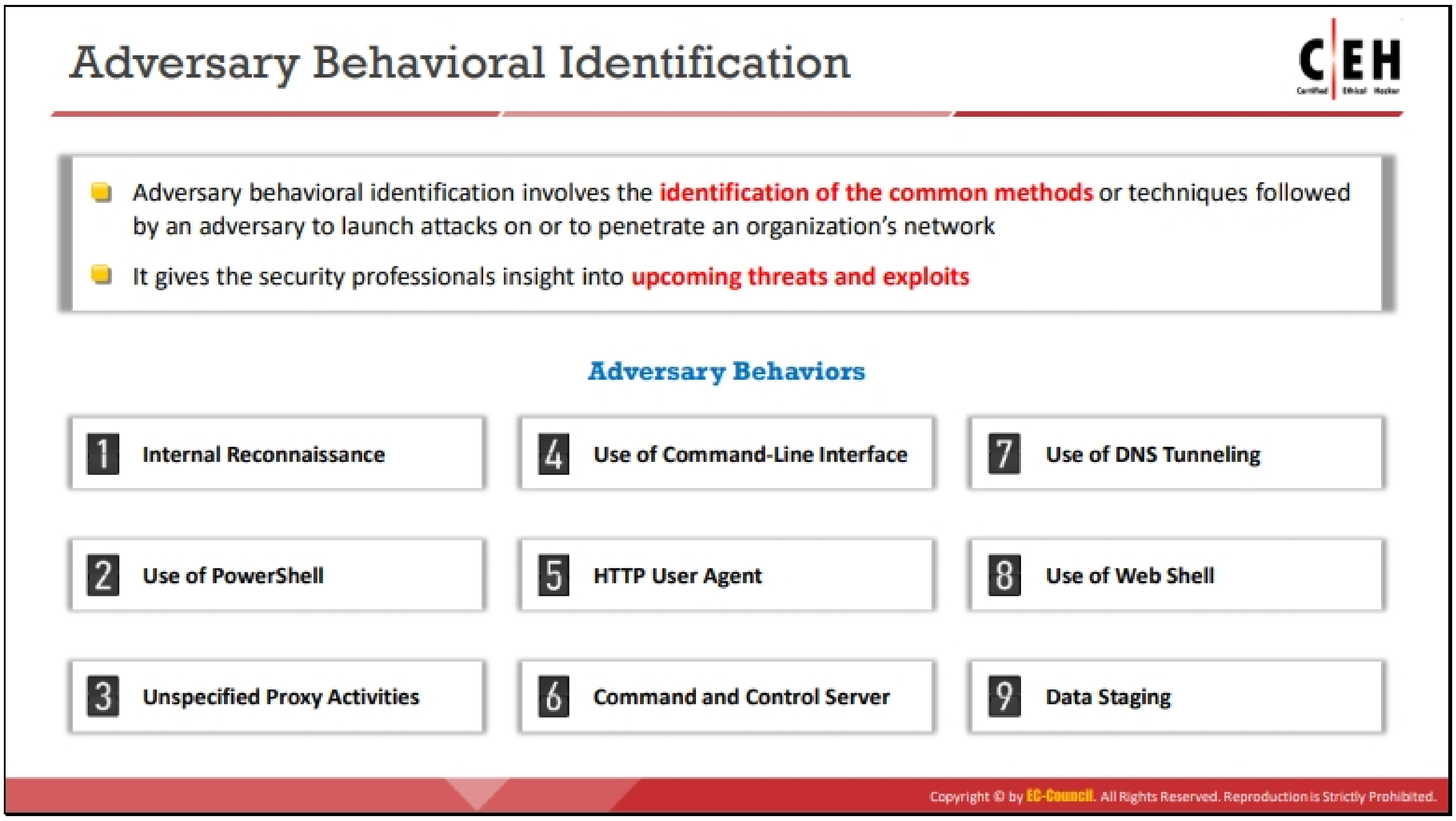
After aggregating the techniques used in all the stages of an attack, the organization can use the information to profile the threat actors. In order to make an accurate attribution of threat actors, the organization must observe all the techniques used by its adversaries.

- **Procedures**

  "Procedures" involve a sequence of actions performed by the threat actors to execute different steps of an attack life cycle. The number of actions usually differs depending upon the objectives of the procedure and the APT group. An advanced threat actor uses advanced procedures that consist of more actions than a normal procedure to achieve the same intermediate result. This is done mainly to increase the success rate of an attack and decrease the probability of detection by security mechanisms.

  For example, in a basic procedure of information gathering, an actor collects information about the target organization; identifies key targets, employees; collects their contact details, identifies vulnerable systems and potential entry points to the target network, and documents all the collected information. The further actions of an adversary depend on the tactics used. These actions include extensive research and repeated information gathering to collect in-depth and up-to-date information on the target individuals via social networking sites. This information can assist threat actors in performing spear phishing, monitoring security controls to identify zero-day exploits in the target systems, and other tasks. For example, a threat actor using a more detailed procedure executes the malware payload. At the time of execution, the malicious code decrypts itself, evades security monitoring controls, deploys persistence, and establishes a command and control channel for communicating with the victim system. This type of procedure is common for malware, where different threat actors may implement the same feature, and hence it is useful in forensic investigations.

An understanding and proper analysis of the procedures followed by certain threat actors during an attack helps organizations profile threat actors. In the initial stage of an attack, such as during information gathering, observing the procedure of an APT group is difficult. However, the later stages of an attack can leave trails that may be used to understand the procedures the attacker followed.



Adversary Behavioral Identification

- Adversary behavioral identification involves the **identification of the common methods** or techniques followed by an adversary to launch attacks on or to penetrate an organization's network
- It gives the security professionals insight into **upcoming threats and exploits**

Adversary Behaviors

1. **Internal Reconnaissance**
2. **Use of PowerShell**
3. **Unspecified Proxy Activities**
4. **Use of Command-Line Interface**
5. **HTTP User Agent**
6. **Command and Control Server**
7. **Use of DNS Tunneling**
8. **Use of Web Shell**
9. **Data Staging**

Adversary Behavioral Identification

Adversary behavioral identification involves the identification of the common methods or techniques followed by an adversary to launch attacks to penetrate an organization's network. It gives security professionals insight into upcoming threats and exploits. It helps them plan network security infrastructure and adapt a range of security procedures as prevention against various cyberattacks.

Given below are some of the behaviors of an adversary that can be used to enhance the detection capabilities of security devices:

- **Internal Reconnaissance**

  Once the adversary is inside the target network, they follow various techniques and methods to carry out internal reconnaissance. This includes the enumeration of systems, hosts, processes, the execution of various commands to find out information such as the local user context and system configuration, hostname, IP addresses, active remote systems, and programs running on the target systems. Security professionals can monitor the activities of an adversary by checking for unusual commands executed in the Batch scripts and PowerShell and by using packet capturing tools.

- **Use of PowerShell**

  PowerShell can be used by an adversary as a tool for automating data exfiltration and launching further attacks. To identify the misuse of PowerShell in the network, security professionals can check PowerShell's transcript logs or Windows Event logs. The user agent string and IP addresses can also be used to identify malicious hosts who try to exfiltrate data.

- **Unspecified Proxy Activities**

  An adversary can create and configure multiple domains pointing to the same host, thus, allowing an adversary to switch quickly between the domains to avoid detection. Security professionals can find unspecified domains by checking the data feeds that are generated by those domains. Using this data feed, the security professionals can also find any malicious files downloaded and the unsolicited communication with the outside network based on the domains.

- **Use of Command-Line Interface**

  On gaining access to the target system, an adversary can make use of the command-line interface to interact with the target system, browse the files, read file content, modify file content, create new accounts, connect to the remote system, and download and install malicious code. Security professionals can identify this behavior of an adversary by checking the logs for process ID, processes having arbitrary letters and numbers, and malicious files downloaded from the Internet.

- **HTTP User Agent**

  In HTTP-based communication, the server identifies the connected HTTP client using the user agent field. An adversary modifies the content of the HTTP user agent field to communicate with the compromised system and to carry further attacks. Therefore, security professionals can identify this attack at an initial stage by checking the content of the user agent field.

- **Command and Control Server**

  Adversaries use command and control servers to communicate remotely with compromised systems through an encrypted session. Using this encrypted channel, the adversary can steal data, delete data, and launch further attacks. Security professionals can detect compromised hosts or networks by identifying the presence of a command and control server by tracking network traffic for outbound connection attempts, unwanted open ports, and other anomalies.

- **Use of DNS Tunneling**

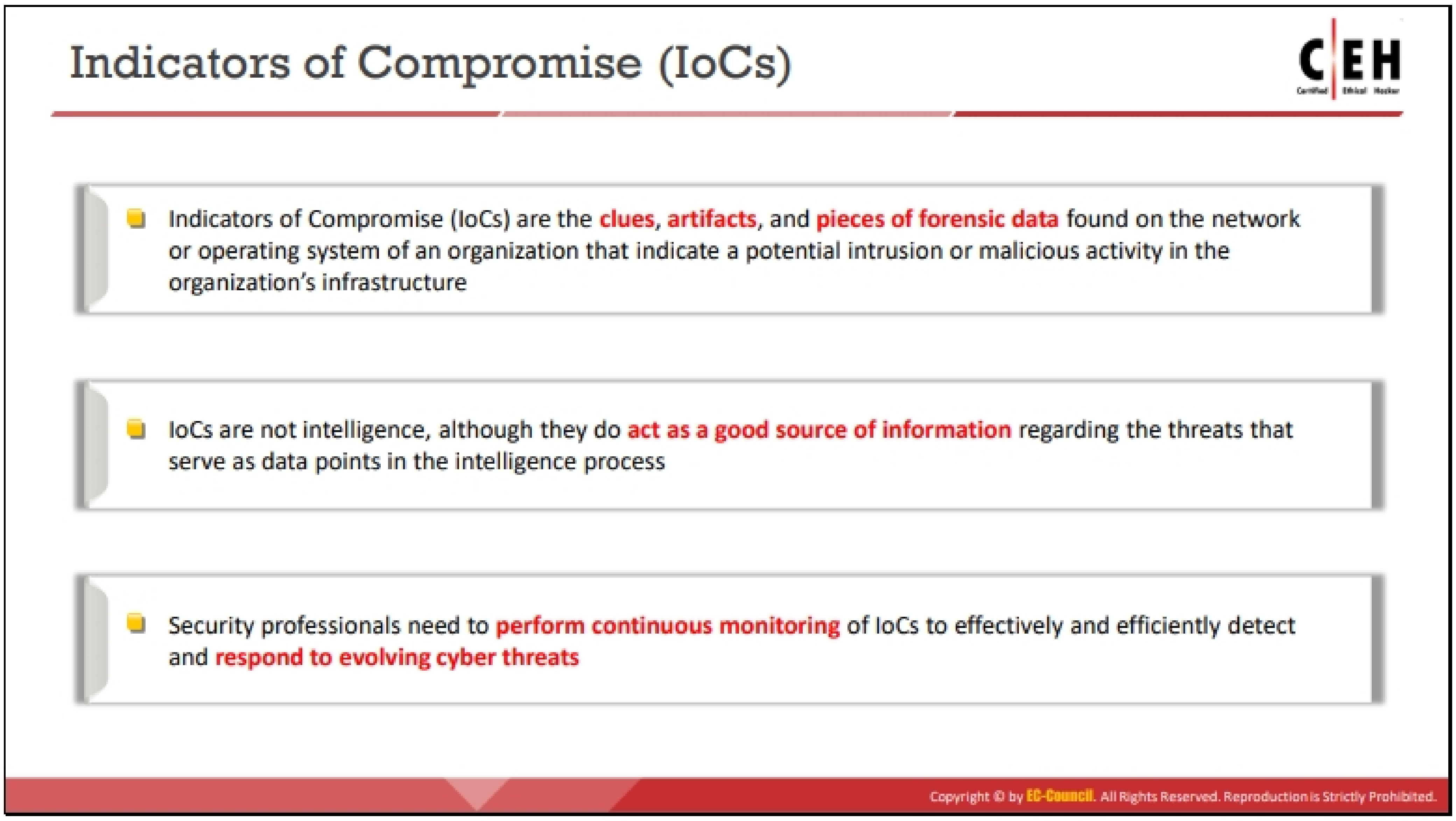
  Adversaries use DNS tunneling to obfuscate malicious traffic in the legitimate traffic carried by common protocols used in the network. Using DNS tunneling, an adversary can also communicate with the command and control server, bypass security controls, and perform data exfiltration. Security professionals can identify DNS tunneling by analyzing malicious DNS requests, DNS payload, unspecified domains, and the destination of DNS requests.

- **Use of Web Shell**

  An adversary uses a web shell to manipulate the web server by creating a shell within a website; it allows an adversary to gain remote access to the functionalities of a server. Using a web shell, an adversary performs various tasks such as data exfiltration, file transfers, and file uploads. Security professionals can identify the web shell running in the network by analyzing server access, error logs, suspicious strings that indicate encoding, user agent strings, and through other methods.

- **Data Staging**

  After successful penetration into a target's network, the adversary uses data staging techniques to collect and combine as much data as possible. The types of data collected by an adversary include sensitive data about the employees and customers, the business tactics of an organization, financial information, and network infrastructure information. Once collected, the adversary can either exfiltrate or destroy the data. Security professionals can detect data staging by monitoring network traffic for malicious file transfers, file integrity monitoring, and event logs.



Indicators of Compromise (IoCs)

- Indicators of Compromise (IoCs) are the **clues**, **artifacts**, and **pieces of forensic data** found on the network or operating system of an organization that indicate a potential intrusion or malicious activity in the organization's infrastructure

- IoCs are not intelligence, although they do **act as a good source of information** regarding the threats that serve as data points in the intelligence process

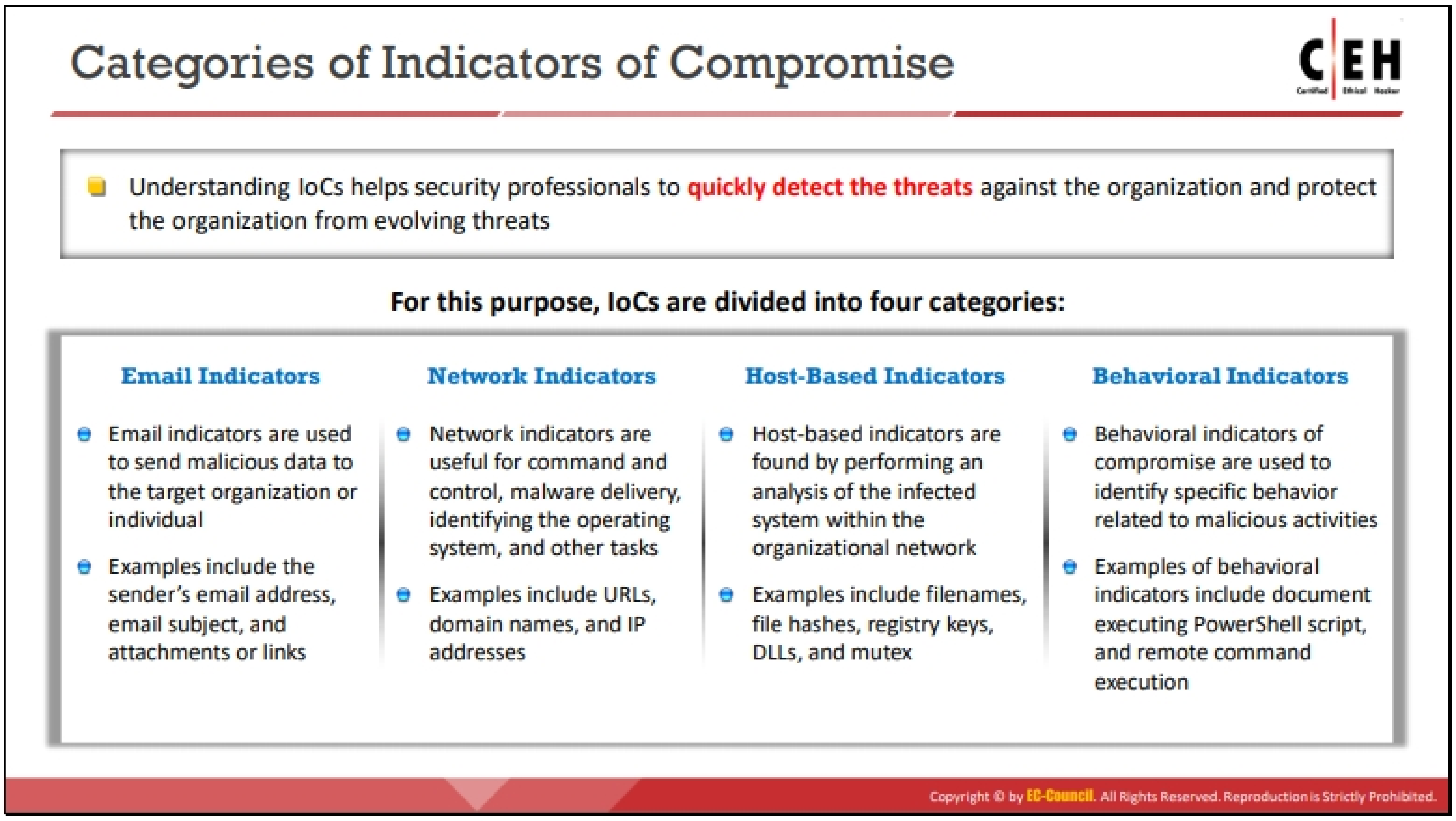
- Security professionals need to **perform continuous monitoring** of IoCs to effectively and efficiently detect and **respond to evolving cyber threats**

Indicators of Compromise (IoCs)

Cyber threats are continuously evolving with the newer TTPs adapted based on the vulnerabilities of the target organization. Security professionals must perform continuous monitoring of IoCs to effectively and efficiently detect and respond to evolving cyber threats. Indicators of Compromise are the clues, artifacts, and pieces of forensic data that are found on a network or operating system of an organization that indicate a potential intrusion or malicious activity in the organization's infrastructure.

However, IoCs are not intelligence; rather, IoCs act as a good source of information about threats that serve as data points in the intelligence process. Actionable threat intelligence extracted from IoCs helps organizations enhance incident-handling strategies. Cybersecurity professionals use various automated tools to monitor IoCs to detect and prevent various security breaches to the organization. Monitoring IoCs also helps security teams enhance the security controls and policies of the organization to detect and block suspicious traffic to thwart further attacks. To overcome the threats associated with IoCs, some organizations like STIX and TAXII have developed standardized reports that contain condensed data related to attacks and shared it with others to leverage the incident response.

An IoC is an atomic indicator, computed indicator, or behavioral indicator. It is the information regarding suspicious or malicious activities that is collected from various security establishments in a network's infrastructure. Atomic indicators are those that cannot be segmented into smaller parts, and whose meaning is not changed in the context of an intrusion. Examples of atomic indicators are IP addresses and email addresses. Computed indicators are obtained from the data extracted from a security incident. Examples of computed indicators are hash values and regular expressions. Behavioral indicators refer to a grouping of both atomic and computed indicators, combined on the basis of some logic.



Categories of Indicators of Compromise

- Understanding IoCs helps security professionals to **quickly detect the threats** against the organization and protect the organization from evolving threats

For this purpose, IoCs are divided into four categories:

Email Indicators

- Email indicators are used to send malicious data to the target organization or individual
- Examples include the sender's email address, email subject, and attachments or links

Network Indicators

- Network indicators are useful for command and control, malware delivery, identifying the operating system, and other tasks
- Examples include URLs, domain names, and IP addresses

Host-Based Indicators

- Host-based indicators are found by performing an analysis of the infected system within the organizational network
- Examples include filenames, file hashes, registry keys, DLLs, and mutex

Behavioral Indicators

- Behavioral indicators of compromise are used to identify specific behavior related to malicious activities
- Examples of behavioral indicators include document executing PowerShell script, and remote command execution

Categories of Indicators of Compromise

The cybersecurity professionals must have proper knowledge about various possible threat actors and their tactics related to cyber threats, mostly called Indicators of Compromise (IoCs). This understanding of IoCs helps security professionals quickly detect the threats entering the organization and protect the organization from evolving threats. For this purpose, IoCs are divided into four categories:

- **Email Indicators**

  Attackers usually prefer email services to send malicious data to the target organization or individual. Such socially engineered emails are preferred due to their ease of use and comparative anonymity. Examples of email indicators include the sender's email address, email subject, and attachments or links.

- **Network Indicators**

  Network indicators are useful for command and control, malware delivery, and identifying details about the operating system, browser type, and other computer-specific information. Examples of network indicators include URLs, domain names, and IP addresses.

- **Host-Based Indicators**

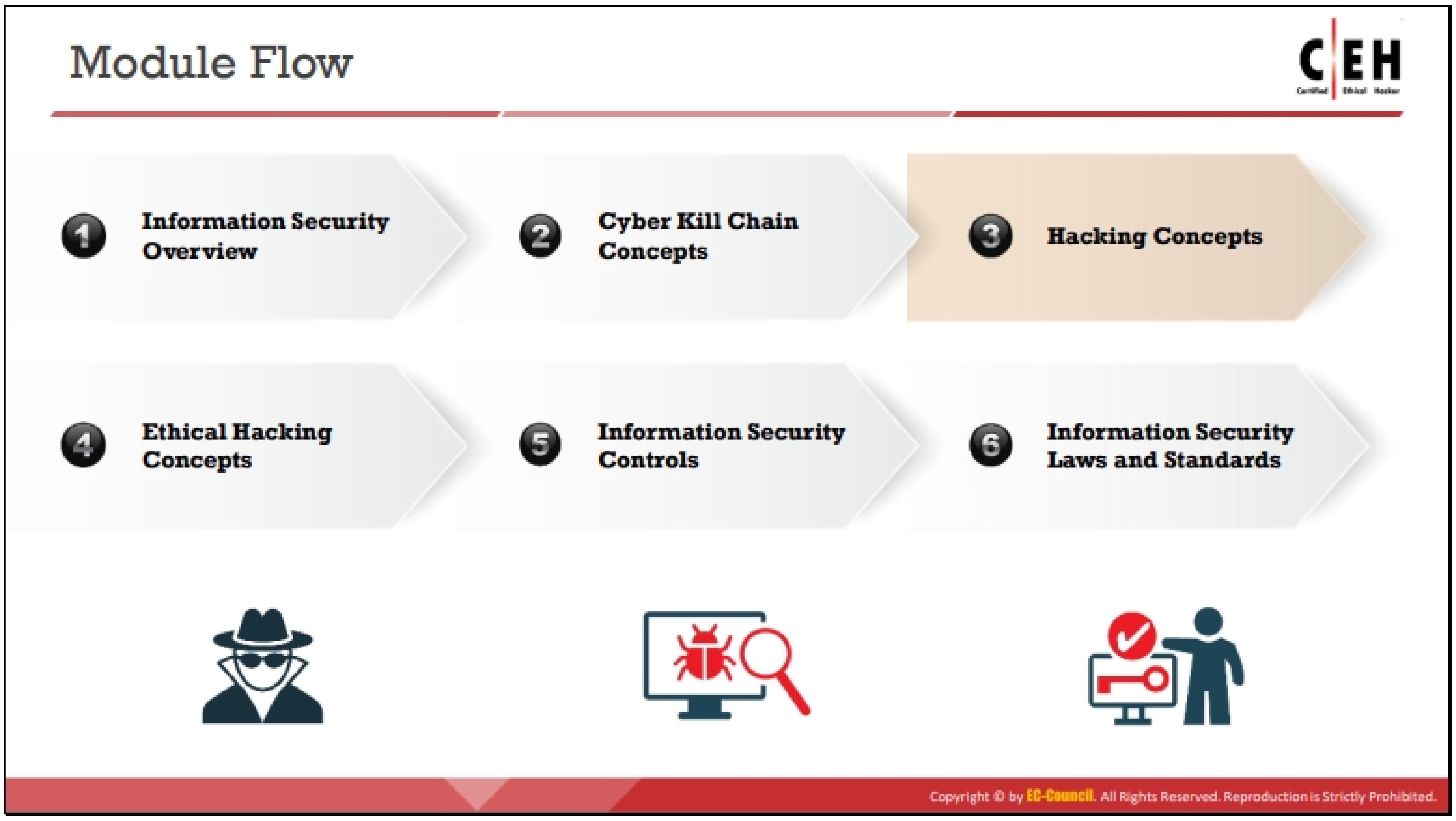
  Host-based indicators are found by performing an analysis of the infected system within the organizational network. Examples of host-based indicators include filenames, file hashes, registry keys, DLLs, and mutex.

- **Behavioral Indicators**

  Generally, typical IoCs are useful for identifying indications of intrusion, such as malicious IP addresses, virus signatures, MD5 hash, and domain names. Behavioral IoCs are used to identify specific behavior related to malicious activities such as code injection into the memory or running the scripts of an application. Well-defined behaviors enable broad protection to block all current and future malicious activities. These indicators are useful to identify when legitimate system services are used for abnormal or unexpected activities. Examples of behavioral indicators include document executing PowerShell script, and remote command execution.

Listed below are some of the key Indicators of Compromise (IoCs):

- Unusual outbound network traffic
- Unusual activity through a privileged user account
- Geographical anomalies
- Multiple login failures
- Increased database read volume
- Large HTML response size
- Multiple requests for the same file
- Mismatched port-application traffic
- Suspicious registry or system file changes
- Unusual DNS requests
- Unexpected patching of systems
- Signs of Distributed Denial-of-Service (DDoS) activity
- Bundles of data in the wrong places
- Web traffic with superhuman behavior

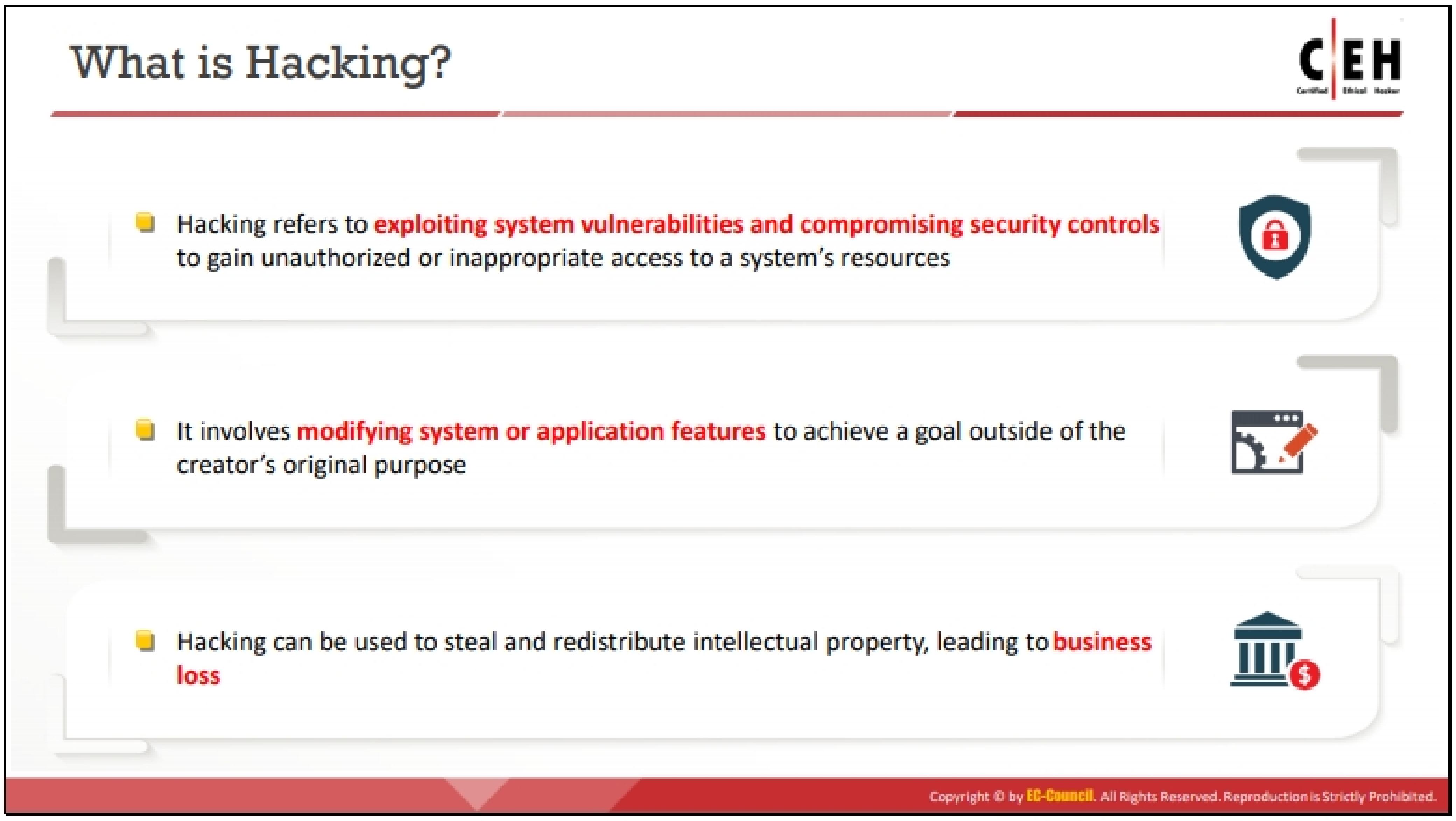


Module Flow

1. **Information Security Overview**
2. **Cyber Kill Chain Concepts**
3. **Hacking Concepts**
4. **Ethical Hacking Concepts**
5. **Information Security Controls**
6. **Information Security Laws and Standards**

Hacking Concepts

This section deals with basic concepts of hacking: what is hacking, who is a hacker, and hacker classes—the five distinct hacking phases that one should be familiar with before proceeding with ethical hacking methodology.



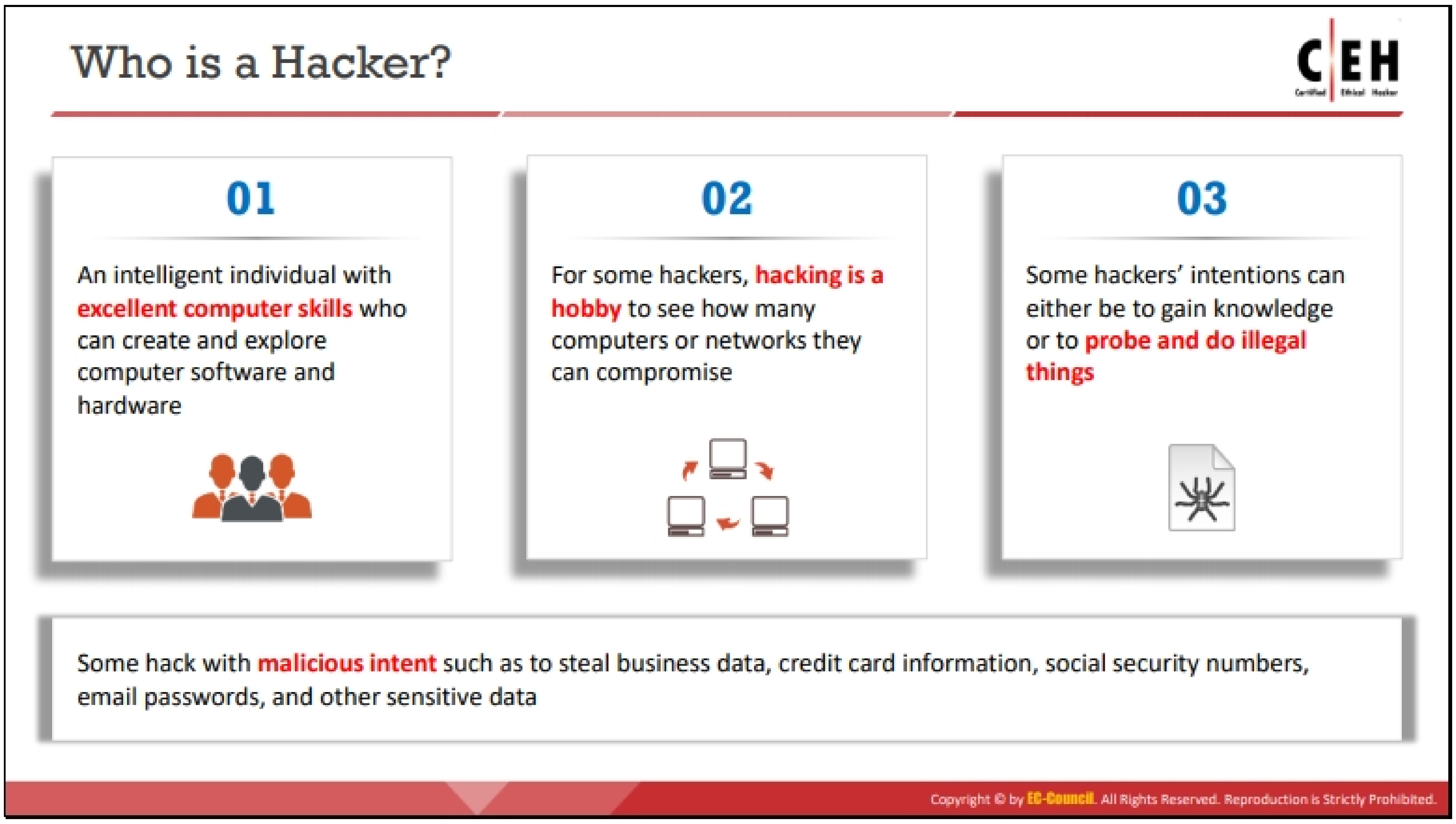
What is Hacking?

- Hacking refers to **exploiting system vulnerabilities and compromising security controls** to gain unauthorized or inappropriate access to a system's resources
- It involves **modifying system or application features** to achieve a goal outside of the creator's original purpose
- Hacking can be used to steal and redistribute intellectual property, leading to **business loss**

What is Hacking?

Hacking in the field of computer security refers to exploiting system vulnerabilities and compromising security controls to gain unauthorized or inappropriate access to system resources. It involves a modifying system or application features to achieve a goal outside its creator's original purpose. Hacking can be done to steal, pilfer, or redistribute intellectual property, thus leading to business loss.

Hacking on computer networks is generally done using scripts or other network programming. Network hacking techniques include creating viruses and worms, performing denial-of-service (DoS) attacks, establishing unauthorized remote access connections to a device using trojans or backdoors, creating botnets, packet sniffing, phishing, and password cracking. The motive behind hacking could be to steal critical information or services, for thrill, intellectual challenge, curiosity, experiment, knowledge, financial gain, prestige, power, peer recognition, vengeance and vindictiveness, among other reasons.



Who is a Hacker?

01

An intelligent individual with **excellent computer skills** who can create and explore computer software and hardware

02

For some hackers, **hacking is a hobby** to see how many computers or networks they can compromise

03

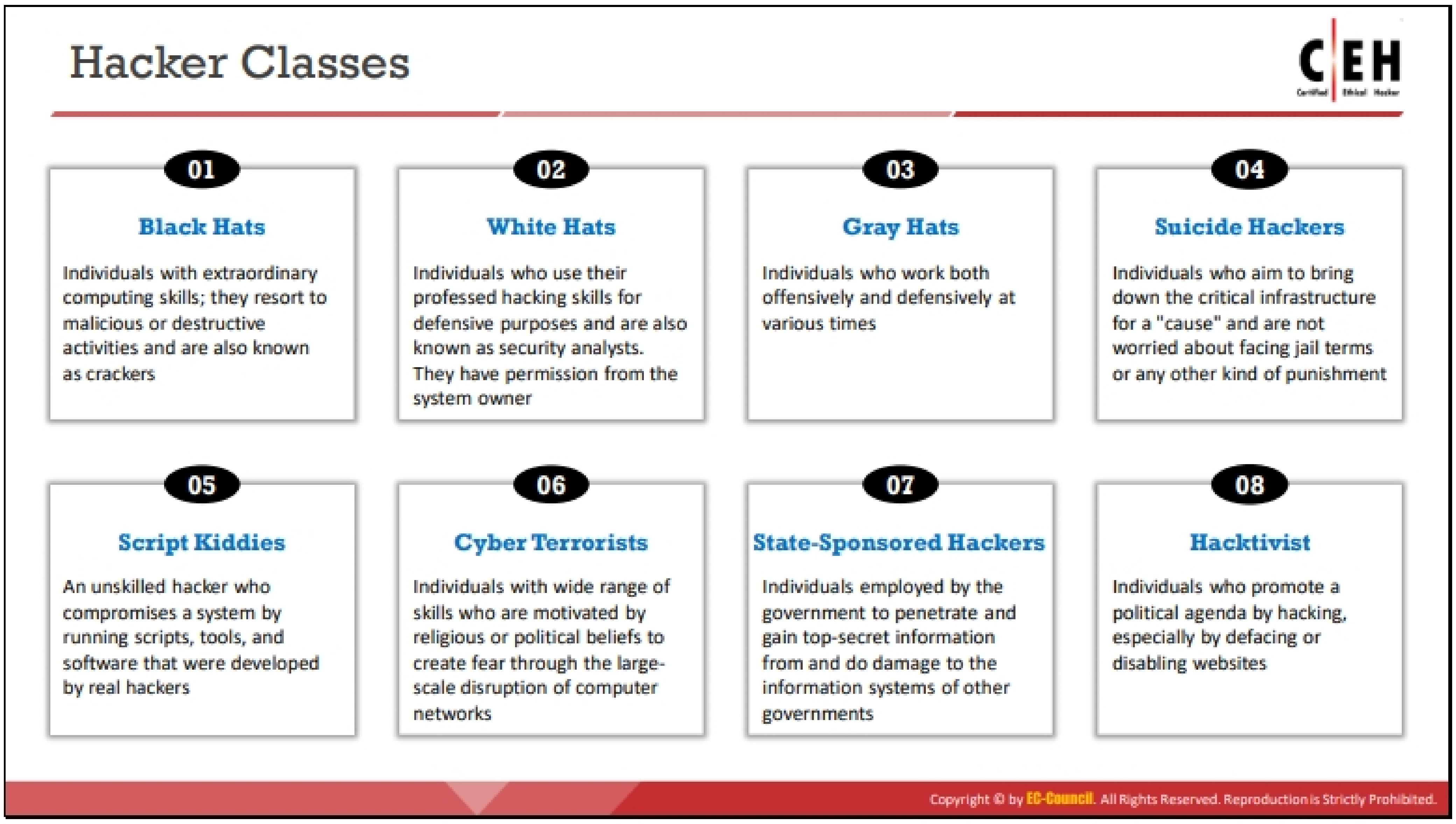
Some hackers' intentions can either be to gain knowledge or to **probe and do illegal things**

Some hack with **malicious intent** such as to steal business data, credit card information, social security numbers, email passwords, and other sensitive data

Who is a Hacker?

A hacker is a person who breaks into a system or network without authorization to destroy, steal sensitive data, or perform malicious attacks. A hacker is an intelligent individual with excellent computer skills, along with the ability to create and explore the computer's software and hardware. Usually, a hacker is a skilled engineer or programmer with enough knowledge to discover vulnerabilities in a target system. They generally have subject expertise and enjoy learning the details of various programming languages and computer systems.

For some hackers, hacking is a hobby to see how many computers or networks they can compromise. Their intention can either be to gain knowledge or to poke around to do illegal things. Some hack with malicious intent behind their escapades, like stealing business data, credit card information, social security numbers, and email passwords.



Hacker Classes

01 **Black Hats**
Individuals with extraordinary computing skills; they resort to malicious or destructive activities and are also known as crackers

02 **White Hats**
Individuals who use their professed hacking skills for defensive purposes and are also known as security analysts. They have permission from the system owner

03 **Gray Hats**
Individuals who work both offensively and defensively at various times

04 **Suicide Hackers**
Individuals who aim to bring down the critical infrastructure for a "cause" and are not worried about facing jail terms or any other kind of punishment

05 **Script Kiddies**
An unskilled hacker who compromises a system by running scripts, tools, and software that were developed by real hackers

06 **Cyber Terrorists**
Individuals with wide range of skills who are motivated by religious or political beliefs to create fear through the large-scale disruption of computer networks

07 **State-Sponsored Hackers**
Individuals employed by the government to penetrate and gain top-secret information from and do damage to the information systems of other governments

08 **Hacktivist**
Individuals who promote a political agenda by hacking, especially by defacing or disabling websites

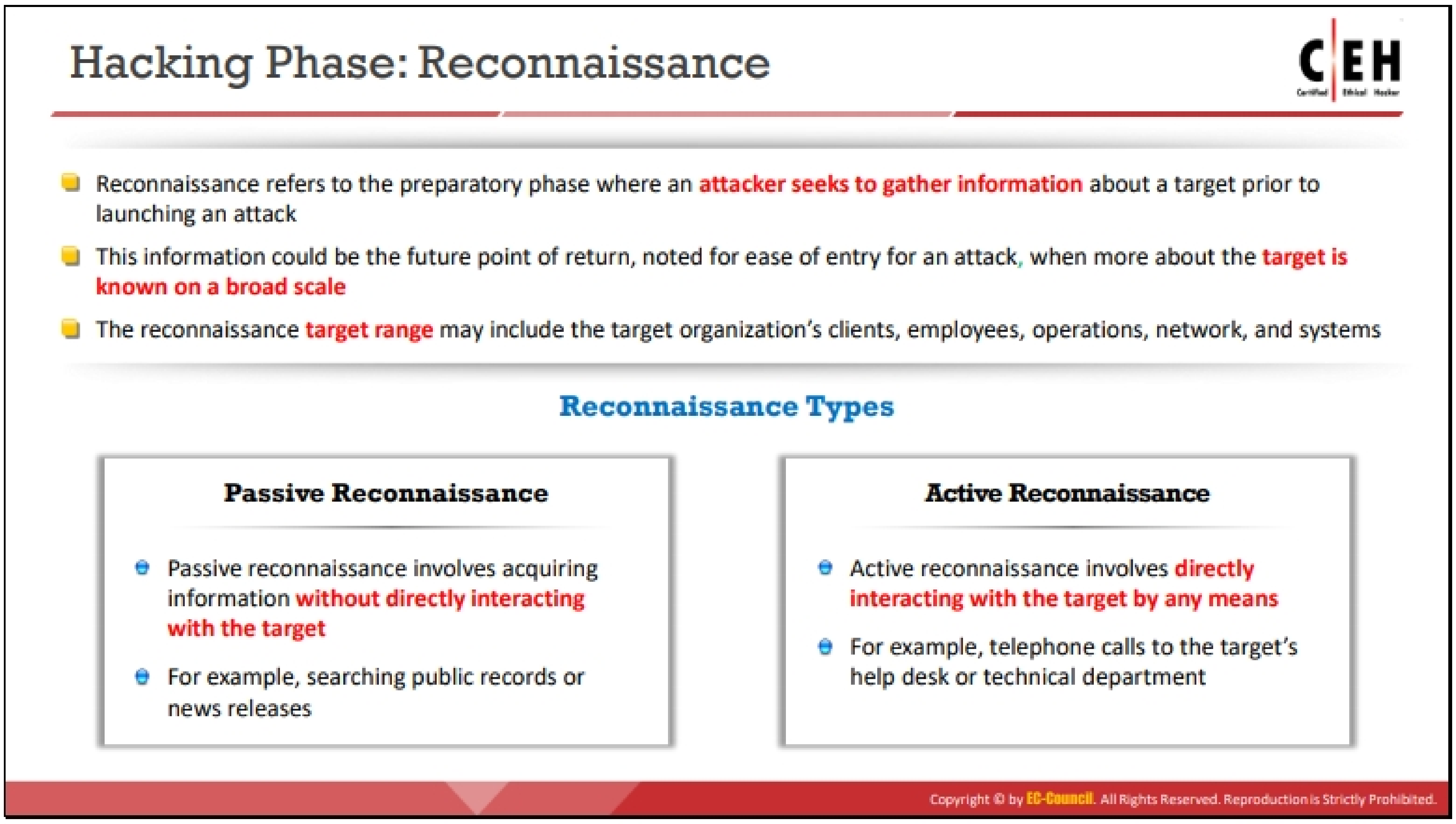
Hacker Classes

Hackers usually fall into one of the following categories, according to their activities:

- **Black Hats**: Black hats are individuals who use their extraordinary computing skills for illegal or malicious purposes. This category of hacker is often involved in criminal activities. They are also known as crackers.
- **White Hats**: White hats or penetration testers are individuals who use their hacking skills for defensive purposes. These days, almost every organization has security analysts who are knowledgeable about hacking countermeasures, which can secure its network and information systems against malicious attacks. They have permission from the system owner.
- **Gray Hats**: Gray hats are the individuals who work both offensively and defensively at various times. Gray hats might help hackers to find various vulnerabilities in a system or network and, at the same time, help vendors to improve products (software or hardware) by checking limitations and making them more secure.
- **Suicide Hackers**: Suicide hackers are individuals who aim to bring down critical infrastructure for a “cause” and are not worried about facing jail terms or any other kind of punishment. Suicide hackers are similar to suicide bombers who sacrifice their life for an attack and are thus not concerned with the consequences of their actions.
- **Script Kiddies**: Script kiddies are unskilled hackers who compromise systems by running scripts, tools, and software developed by real hackers. They usually focus on the quantity rather than the quality of the attacks that they initiate.

- **Cyber Terrorists**: Cyber terrorists are individuals with a wide range of skills, motivated by religious or political beliefs, to create fear of large-scale disruption of computer networks.
- **State-Sponsored Hackers**: State-sponsored hackers are individuals employed by the government to penetrate, gain top-secret information from, and damage the information systems of other governments.
- **Hacktivist**: Hacktivism is when hackers break into government or corporate computer systems as an act of protest. Hacktivists use hacking to increase awareness of their social or political agendas, as well as to boost their own reputations in both the online and offline arenas. They are individuals who use hacking to promote a political agenda, especially by defacing or disabling websites.

  Common hacktivist targets include government agencies, multinational corporations, and any other entity that they perceive as a threat. Irrespective of the hacktivists' intentions, the gaining of unauthorized access is a crime.



Hacking Phase: Reconnaissance

- Reconnaissance refers to the preparatory phase where an **attacker seeks to gather information** about a target prior to launching an attack
- This information could be the future point of return, noted for ease of entry for an attack, when more about the **target is known on a broad scale**
- The reconnaissance **target range** may include the target organization's clients, employees, operations, network, and systems

Reconnaissance Types

Passive Reconnaissance

- Passive reconnaissance involves acquiring information **without directly interacting with the target**
- For example, searching public records or news releases

Active Reconnaissance

- Active reconnaissance involves **directly interacting with the target by any means**
- For example, telephone calls to the target's help desk or technical department

Hacking Phases

In general, there are five phases of hacking:

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Clearing Tracks

Hacking Phase: Reconnaissance

Reconnaissance refers to the preparatory phase in which an attacker gathers as much information as possible about the target prior to launching the attack. In this phase, the attacker draws on competitive intelligence to learn more about the target. It could be the future point of return, noted for ease of entry for an attack when more about the target is known on a broad scale. The reconnaissance target range may include the target organization's clients, employees, operations, network, and systems.

This phase allows attackers to plan the attack. It may take some time as the attacker gathers as much information as possible. Part of this reconnaissance may involve social engineering. A social engineer is a person who convinces people to reveal information such as unlisted phone numbers, passwords, and other sensitive information. For instance, the hacker could call the target's Internet service provider and, using personal information previously obtained, convince the customer service representative that the hacker is actually the target, and in doing so, obtain even more information about the target.

Another reconnaissance technique is dumpster diving. Dumpster diving is, simply enough, looking through an organization's trash for any discarded sensitive information. Attackers can use the Internet to obtain information such as employees' contact information, business partners, technologies currently in use, and other critical business knowledge. Dumpster diving may even provide attackers with even more sensitive information, such as usernames, passwords, credit card statements, bank statements, ATM receipts, Social Security numbers, private telephone numbers, checking account numbers, or other sensitive data.

Searching for the target company's web site in the Internet's Whois database can easily provide hackers with the company's IP addresses, domain names, and contact information.

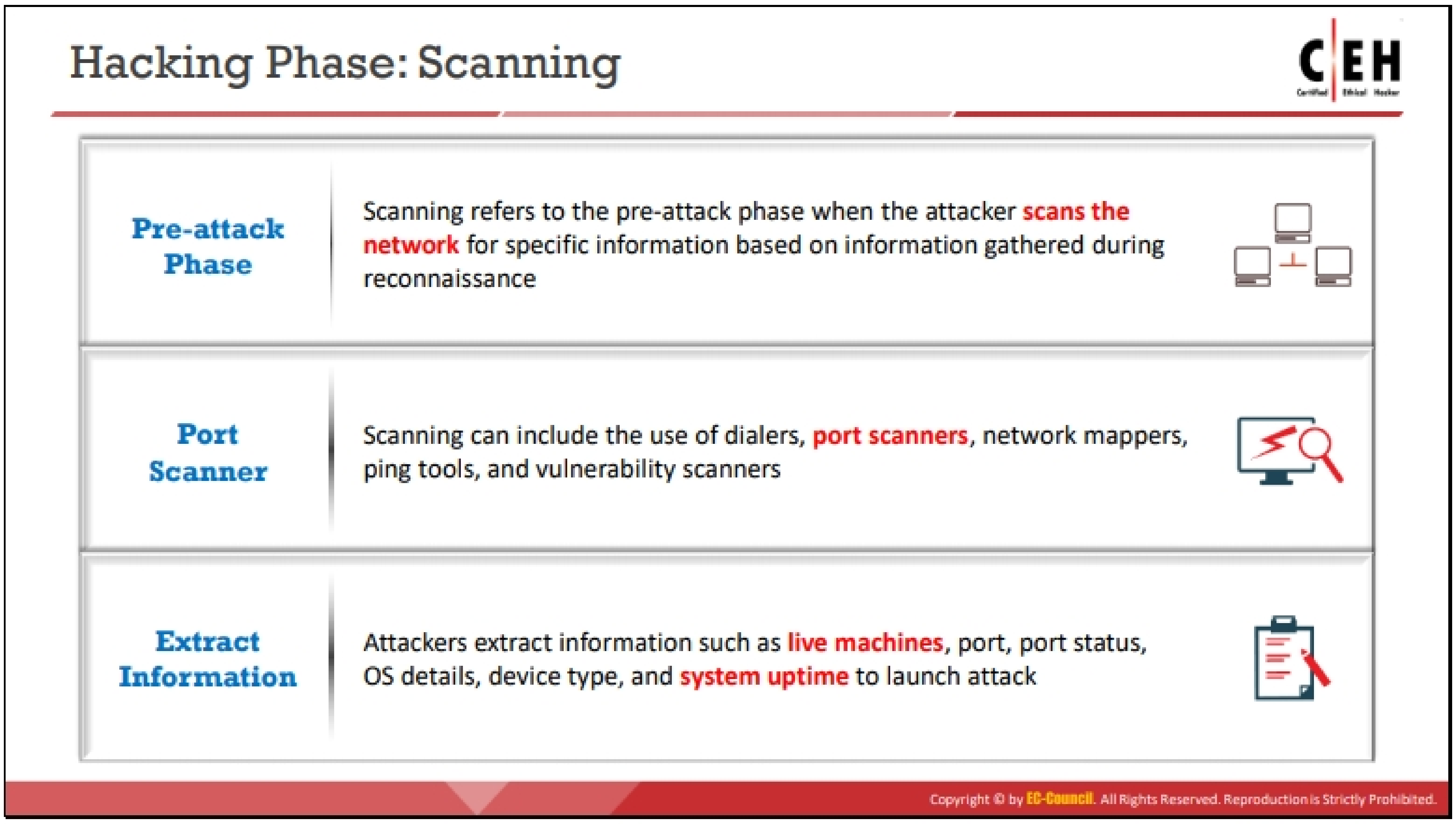
Reconnaissance Types

Reconnaissance techniques are broadly categorized into active and passive.

When an attacker is using passive reconnaissance techniques, they do not interact with the target directly. Instead, the attacker relies on publicly available information, news releases, or other no-contact methods.

Active reconnaissance techniques, on the other hand, involve direct interactions with the target system by using tools to detect open ports, accessible hosts, router locations, network mapping, details of operating systems, and applications. Attackers use active reconnaissance when there is a low probability of the detection of these activities. For example, they may make telephone calls to the help desk or technical department.

As an ethical hacker, it is important to be able to distinguish among the various reconnaissance methods and advocate preventive measures in the light of potential threats. Companies, on their part, must address security as an integral part of their business and operational strategies, and be equipped with the proper policies and procedures to check for potential vulnerabilities.



Hacking Phase: Scanning

Pre-attack Phase	Scanning refers to the pre-attack phase when the attacker **scans the network** for specific information based on information gathered during reconnaissance
Port Scanner	Scanning can include the use of dialers, **port scanners**, network mappers, ping tools, and vulnerability scanners
Extract Information	Attackers extract information such as **live machines**, port, port status, OS details, device type, and **system uptime** to launch attack

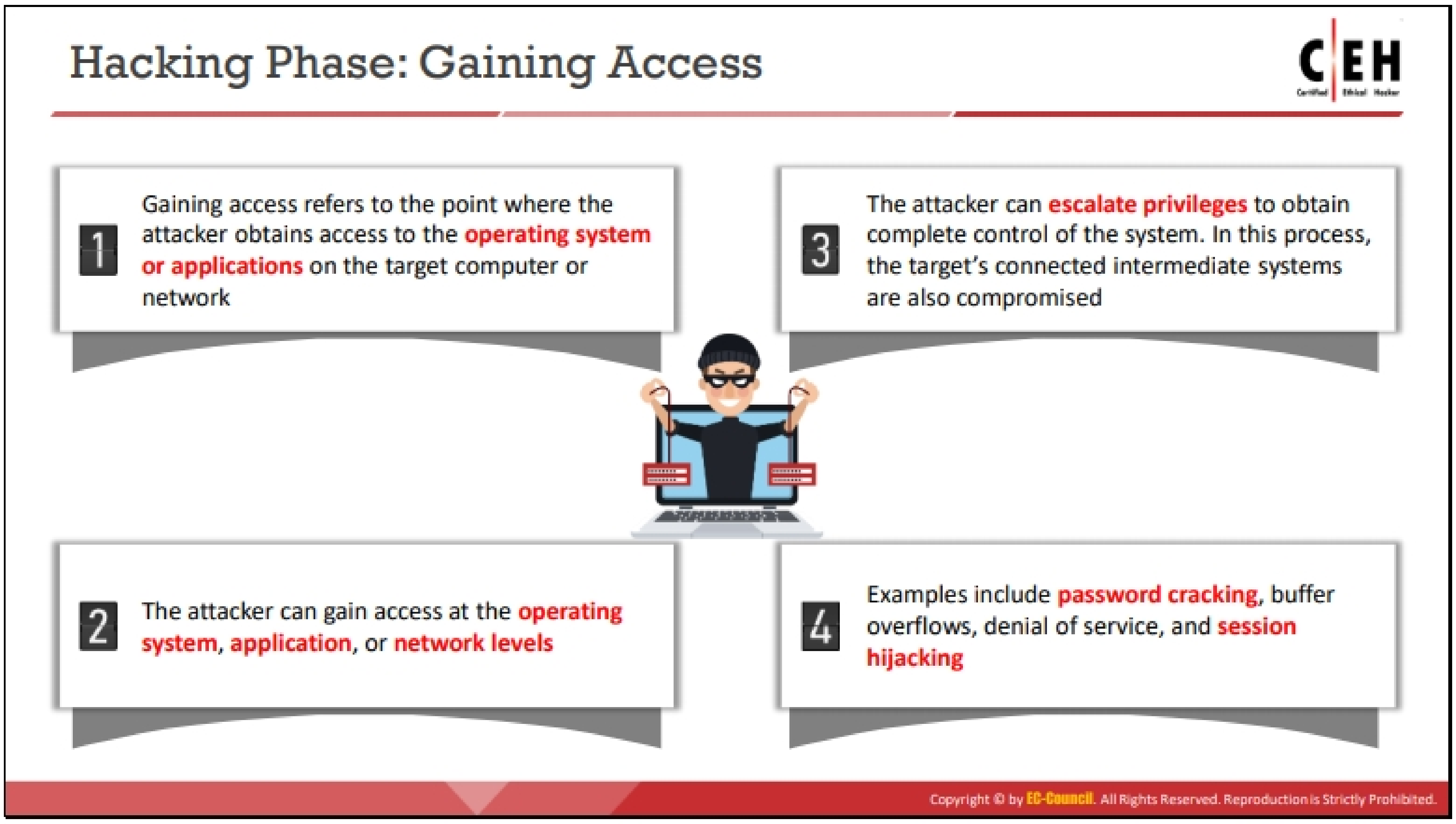
Hacking Phase: Scanning

Scanning is the phase immediately preceding the attack. Here, the attacker uses the details gathered during reconnaissance to scan the network for specific information. Scanning is a logical extension of active reconnaissance, and in fact, some experts do not differentiate scanning from active reconnaissance. There is a slight difference, however, in that scanning involves more in-depth probing on the part of the attacker. Often the reconnaissance and scanning phases overlap, and it is not always possible to separate the two. An attacker can gather critical network information such as the mapping of systems, routers, and firewalls by using simple tools such as the standard Windows utility Traceroute. Alternatively, they can use tools such as Cheops to add additional information to Traceroute's results.

Scanning can include the use of dialers, port scanners, network mappers, ping tools, vulnerability scanners, or other tools. Attackers extract information such as live machines, port, port status, OS details, device type, and system uptime to launch an attack.

Port scanners detect listening ports to find information about the nature of services running on the target machine. The primary defense technique against port scanners is shutting down services that are not required and implementing appropriate port filtering. However, attackers can still use tools to determine the rules implemented by the port filtering.

The most commonly used tools are vulnerability scanners, which can search for thousands of known vulnerabilities on a target network. This gives the attacker an advantage because he or she only has to find a single means of entry, while the systems professional has to secure as much vulnerability as possible by applying patches. Organizations that use intrusion detection systems still have to remain vigilant because attackers can and will use evasion techniques wherever possible.



Hacking Phase: Gaining Access

C|EH
Certified Ethical Hacker

1 Gaining access refers to the point where the attacker obtains access to the **operating system or applications** on the target computer or network

2 The attacker can gain access at the **operating system**, **application**, or **network levels**

3 The attacker can **escalate privileges** to obtain complete control of the system. In this process, the target's connected intermediate systems are also compromised

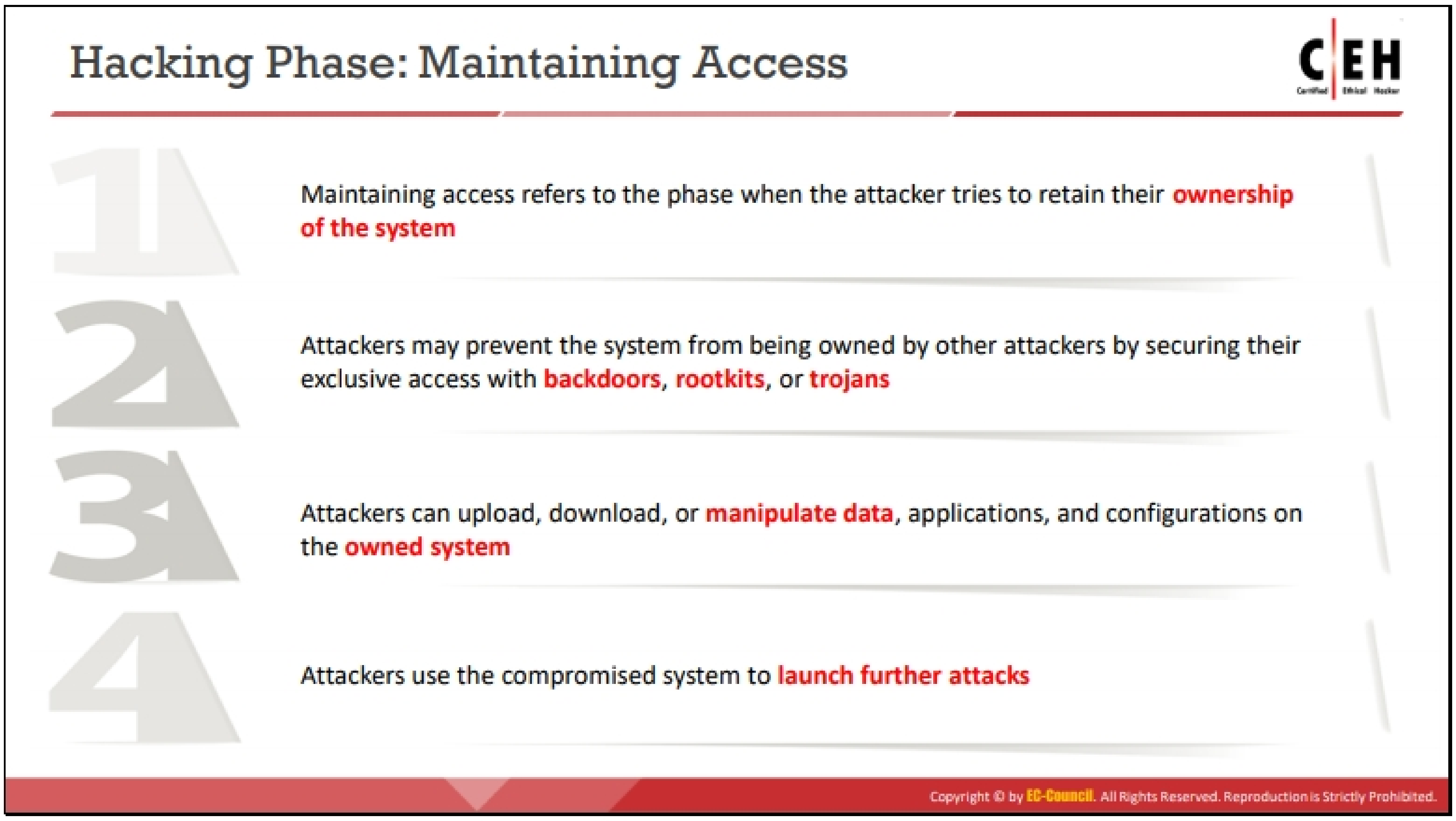
4 Examples include **password cracking**, buffer overflows, denial of service, and **session hijacking**

Hacking Phase: Gaining Access

This is the phase in which real hacking occurs. Attackers use vulnerabilities identified during the reconnaissance and scanning phases to gain access to the target system and network. Gaining access refers to the point where the attacker obtains access to the operating system or to applications on the computer or network. The attacker can gain access to the operating system, application, or network level. Even though attackers can cause plenty of damage without gaining any access to the system, the impact of unauthorized access is catastrophic. For instance, external denial-of-service attacks can either exhaust resources or stop services from running on the target system. Ending processes can stop a service, using a logic bomb or time bomb, or even reconfigure and crash the system. Furthermore, attackers can exhaust system and network resources by consuming all outgoing communication links.

Attackers gain access to the target system locally (offline), over a LAN, or the Internet. Examples include password cracking, stack-based buffer overflows, denial-of-service, and session hijacking. Using a technique called spoofing to exploit the system by pretending to be a legitimate user or different system, attackers can send a data packet containing a bug to the target system in order to exploit a vulnerability. Packet flooding also breaks the availability of essential services. Smurf attacks attempt to cause users on a network to flood each other with data, making it appear as if everyone is attacking each other, and leaving the hacker anonymous.

A hacker's chances of gaining access to a target system depend on several factors such as the architecture and configuration of the target system, the skill level of the perpetrator, and the initial level of access obtained. Once an attacker gains access to the target system, they then try to escalate privileges in order to take complete control. In the process, they also compromise the intermediate systems that are connected to it.



Hacking Phase: Maintaining Access

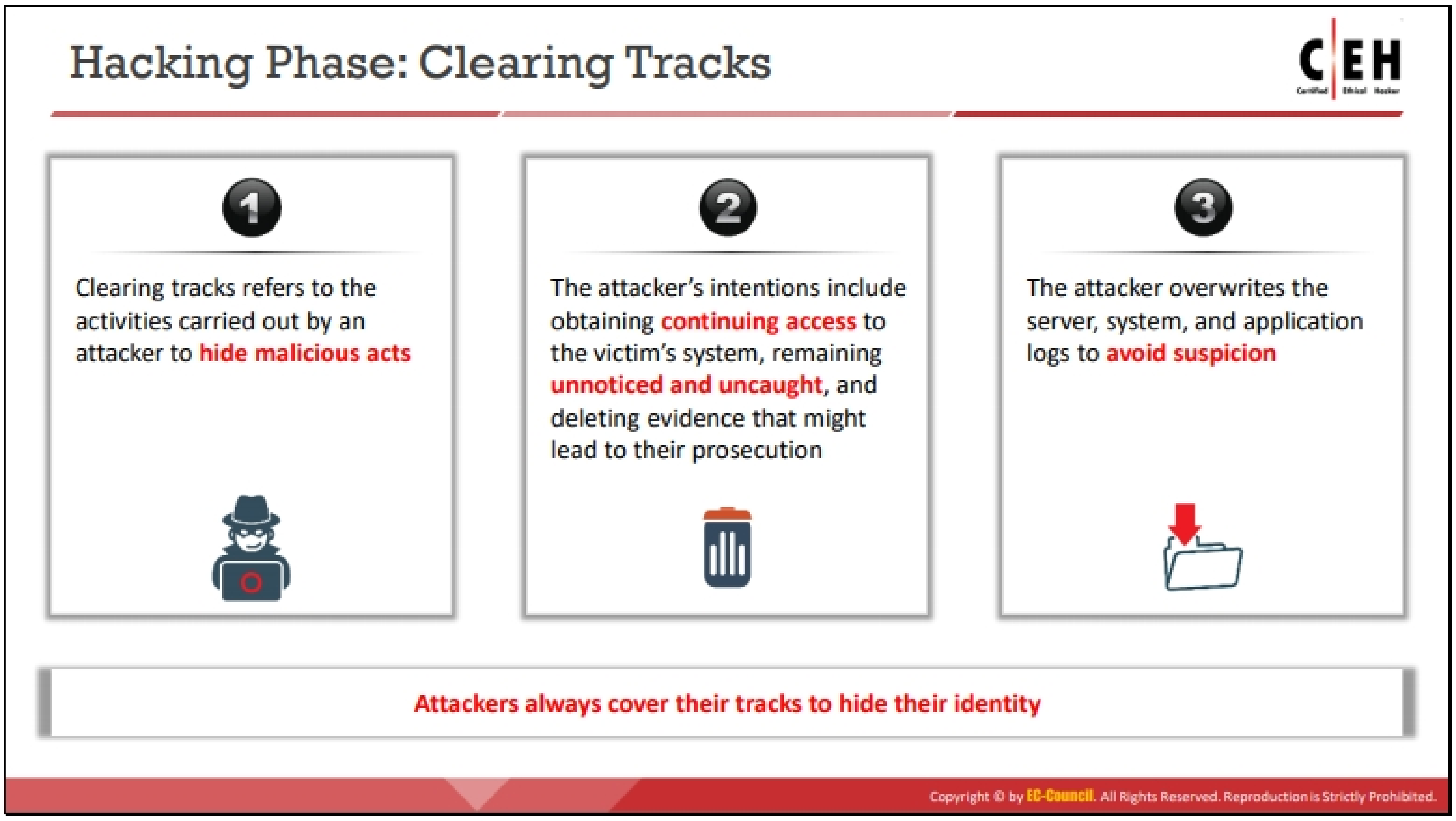
1. Maintaining access refers to the phase when the attacker tries to retain their **ownership of the system**
2. Attackers may prevent the system from being owned by other attackers by securing their exclusive access with **backdoors**, **rootkits**, or **trojans**
3. Attackers can upload, download, or **manipulate data**, applications, and configurations on the **owned system**
4. Attackers use the compromised system to **launch further attacks**

Hacking Phase: Maintaining Access

Maintaining access refers to the phase when the attacker tries to retain his or her ownership of the system. Once an attacker gains access to the target system with admin or root-level privileges (thus owning the system), they can use both the system and its resources at will. The attacker can either use the system as a launchpad to scan and exploit other systems or to keep a low profile and continue their exploitation. Both of these actions can cause a great amount of damage. For instance, the hacker could implement a sniffer to capture all network traffic, including Telnet and FTP (file transfer protocol) sessions with other systems, and then transmit that data wherever they please.

Attackers who choose to remain undetected remove evidence of their entry and install a backdoor or a trojan to gain repeat access. They can also install rootkits at the kernel level to gain full administrative access to the target computer. Rootkits gain access at the operating system level, while trojans gain access at the application level. Both rootkits and trojans require users to install them locally. In Windows systems, most trojans install themselves as a service and run as part of the local system with administrative access.

Attackers can upload, download, or manipulate data, applications, and configurations on the owned system and can also use trojans to transfer usernames, passwords, and any other information stored on the system. They can maintain control over the system for a long time by closing up vulnerabilities to prevent other hackers from taking control of them, and sometimes, in the process, render some degree of protection to the system from other attacks. Attackers use the compromised system to launch further attacks.



Hacking Phase: Clearing Tracks

1

Clearing tracks refers to the activities carried out by an attacker to **hide malicious acts**

2

The attacker's intentions include obtaining **continuing access** to the victim's system, remaining **unnoticed and uncaught**, and deleting evidence that might lead to their prosecution

3

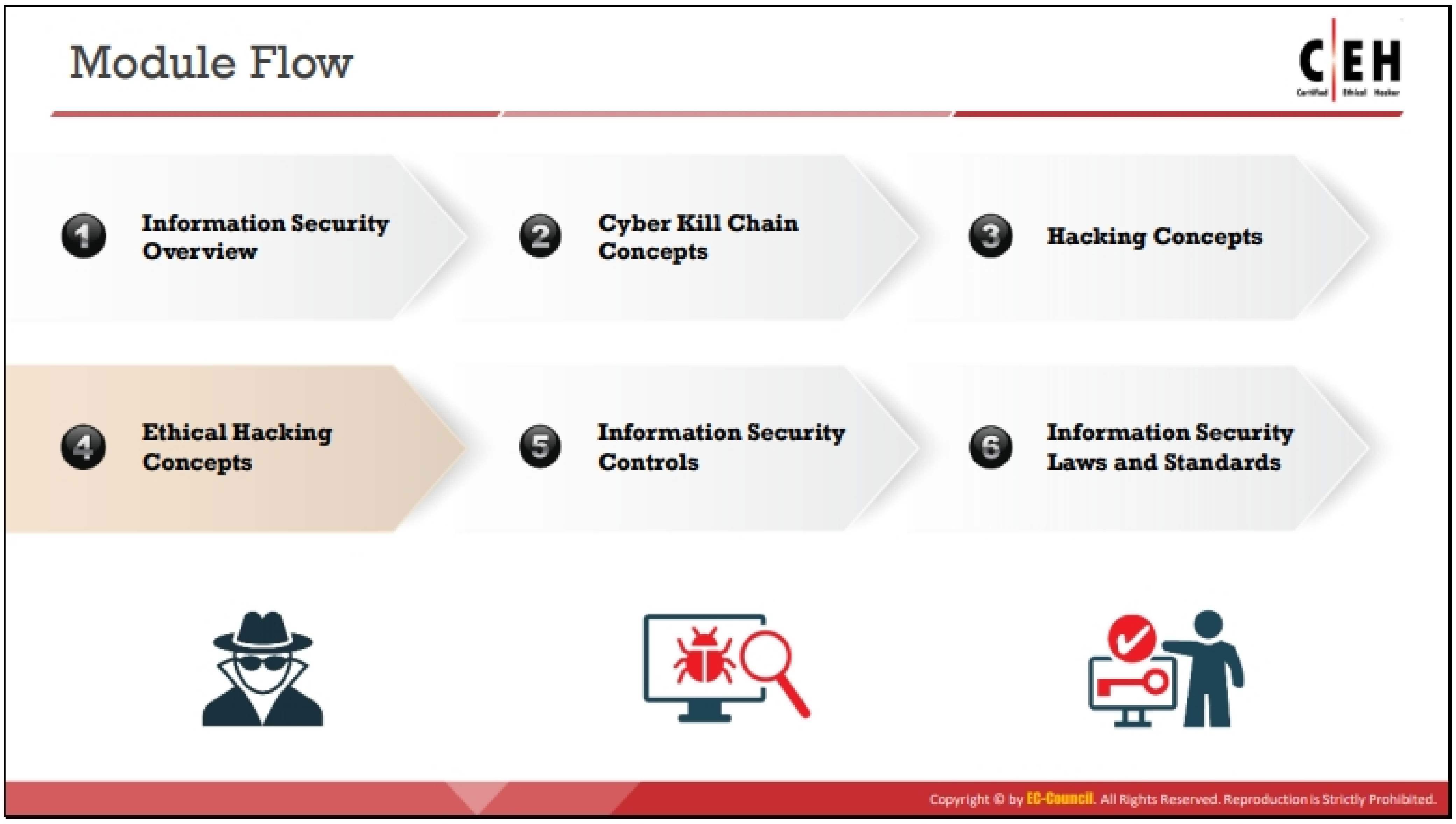
The attacker overwrites the server, system, and application logs to **avoid suspicion**

Attackers always cover their tracks to hide their identity

Hacking Phase: Clearing Tracks

For obvious reasons, such as avoiding legal trouble and maintaining access, attackers will usually attempt to erase all evidence of their actions. Clearing tracks refers to the activities carried out by an attacker to hide malicious acts. The attacker's intentions include continuing access to the victim's system, remaining unnoticed and uncaught, and deleting evidence that might lead to their own prosecution. They use utilities such as PsTools (*https://docs.microsoft.com*), Netcat, or trojans to erase their footprints from the system's log files. Once the trojans are in place, the attacker has most likely gained total control of the system and can execute scripts in the trojan or rootkit to replace the critical system and log files to hide their presence in the system. Attackers always cover their tracks to hide their identity.

Other techniques include steganography and tunneling. Steganography is the process of hiding data in other data, for instance, in image and sound files. Tunneling takes advantage of the transmission protocol by carrying one protocol over another. Attackers can use even a small amount of extra space in the data packet's TCP and IP headers to hide information. An attacker can use the compromised system to launch new attacks against other systems or as a means of reaching another system on the network undetected. Thus, this phase of the attack can turn into another attack's reconnaissance phase. System administrators can deploy host-based IDS (intrusion detection systems) and antivirus software in order to detect trojans and other seemingly compromised files and directories. An ethical hacker must be aware of the tools and techniques that attackers deploy so that they can advocate and implement the countermeasures detailed in subsequent modules.



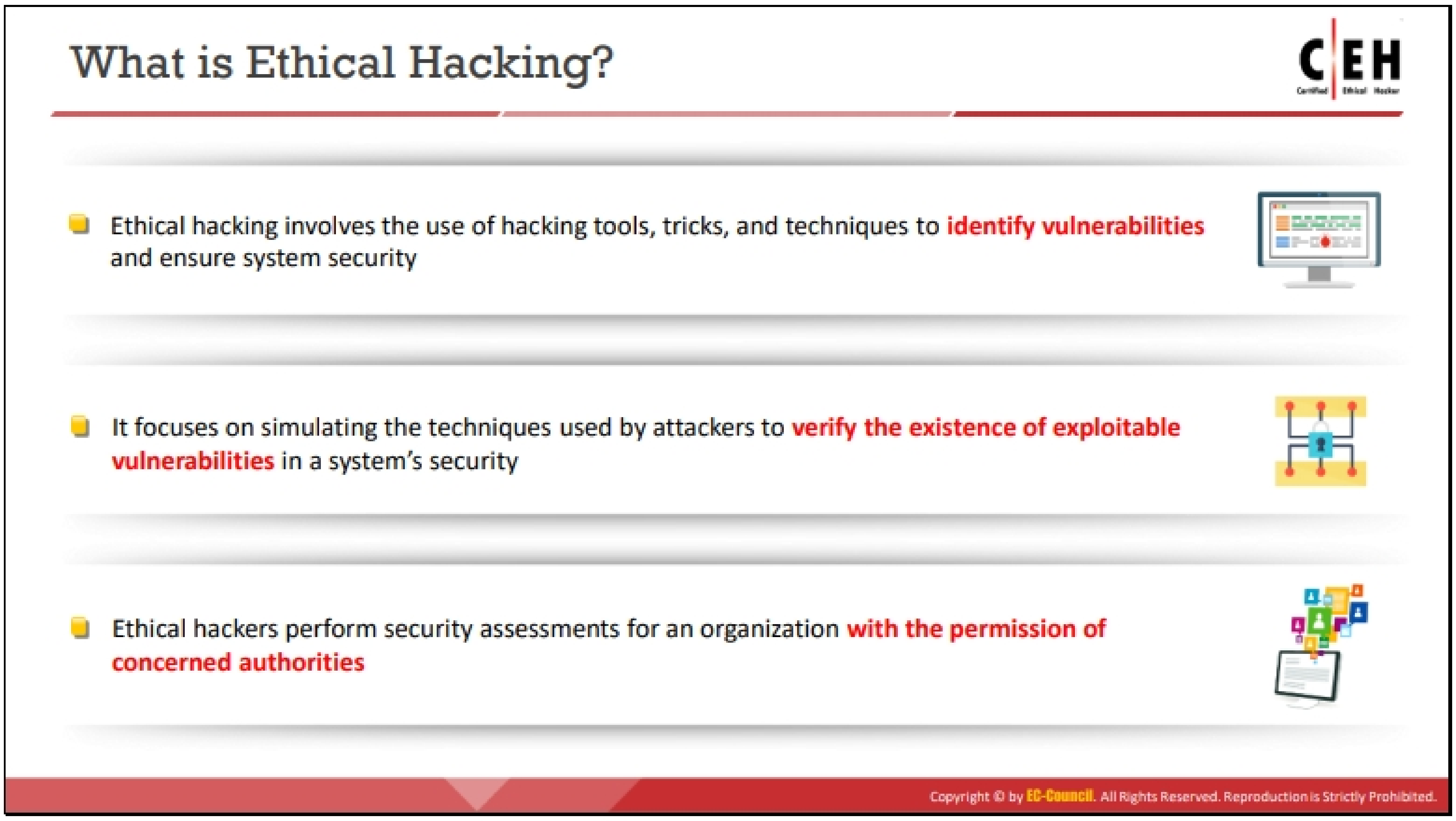
Module Flow

1. Information Security Overview
2. Cyber Kill Chain Concepts
3. Hacking Concepts
4. Ethical Hacking Concepts
5. Information Security Controls
6. Information Security Laws and Standards

Ethical Hacking Concepts

An ethical hacker follows processes similar to those of a malicious hacker. The steps to gain and maintain access to a computer system are similar irrespective of the hacker’s intentions.

This section provides an overview of ethical hacking, why ethical hacking is necessary, the scope and limitations of ethical hacking, and the skills of an ethical hacker.



What is Ethical Hacking?

- Ethical hacking involves the use of hacking tools, tricks, and techniques to **identify vulnerabilities** and ensure system security
- It focuses on simulating the techniques used by attackers to **verify the existence of exploitable vulnerabilities** in a system's security
- Ethical hackers perform security assessments for an organization **with the permission of concerned authorities**

What is Ethical Hacking?

Ethical hacking is the practice of employing computer and network skills in order to assist organizations in testing their network security for possible loopholes and vulnerabilities. White Hats (also known as security analysts or ethical hackers) are the individuals or experts who perform ethical hacking. Nowadays, most organizations (such as private companies, universities, and government organizations) are hiring White Hats to assist them in enhancing their cybersecurity. They perform hacking in ethical ways, with the permission of the network or system owner and without the intention to cause harm. Ethical hackers report all vulnerabilities to the system and network owner for remediation, thereby increasing the security of an organization's information system. Ethical hacking involves the use of hacking tools, tricks, and techniques typically used by an attacker to verify the existence of exploitable vulnerabilities in system security.

Today, the term hacking is closely associated with illegal and unethical activities. There is continuing debate as to whether hacking can be ethical or not, given the fact that unauthorized access to any system is a crime. Consider the following definitions:

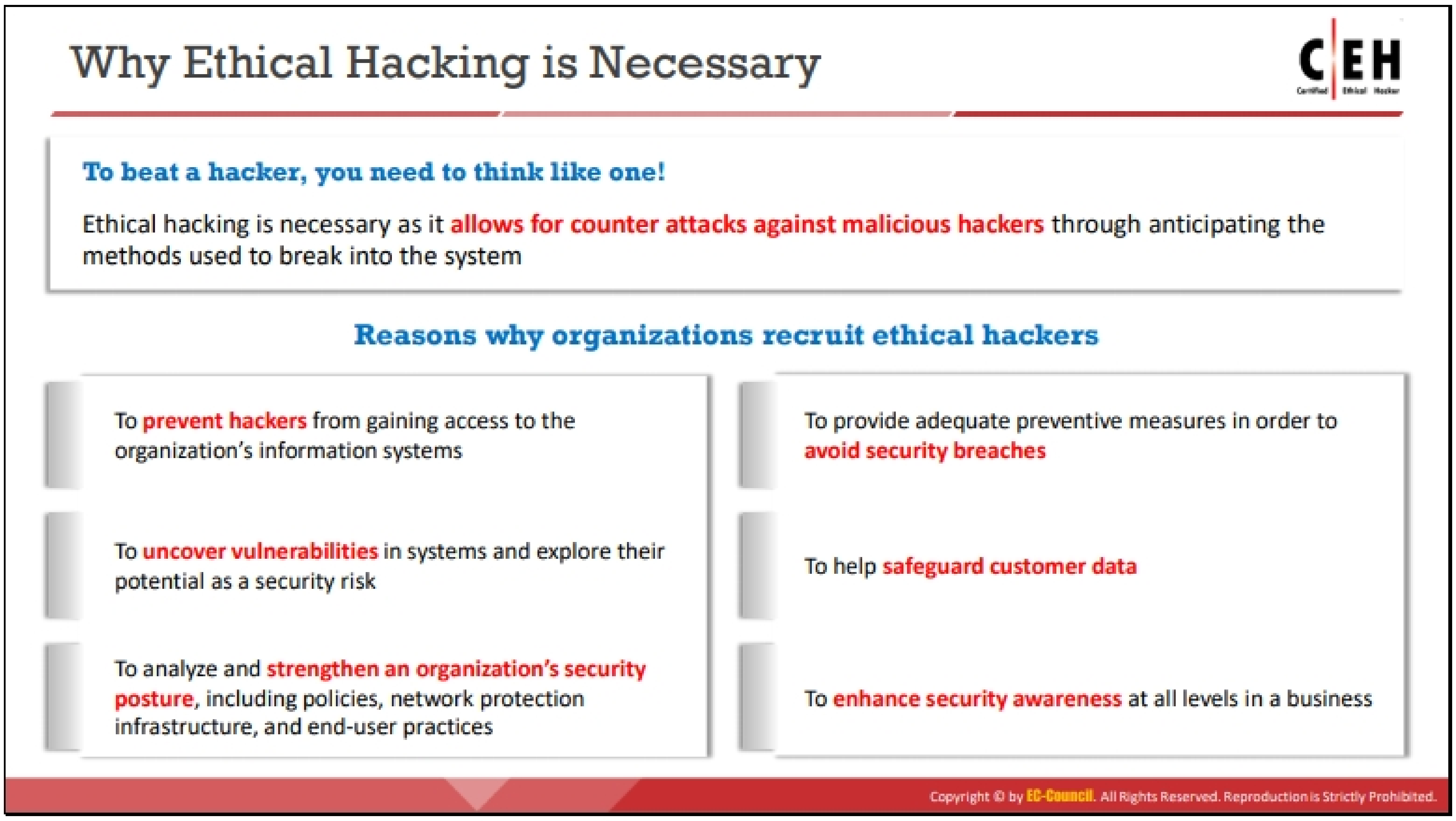
- The noun "hacker" refers to a person who enjoys learning the details of computer systems and stretching their capabilities.
- The verb "to hack" describes the rapid development of new programs or the reverse engineering of existing software to make it better or more efficient in new and innovative ways.
- The terms "cracker" and "attacker" refer to persons who employ their hacking skills for offensive purposes.

- The term “ethical hacker” refers to security professionals who employ their hacking skills for defensive purposes.

Most companies employ IT professionals to audit their systems for known vulnerabilities. Although this is a beneficial practice, crackers are usually more interested in using newer, lesser-known vulnerabilities, and so these by-the-numbers system audits do not suffice. A company needs someone who can think like a cracker, keep up with the newest vulnerabilities and exploits, and recognize potential vulnerabilities where others cannot. This is the role of the ethical hacker.

Ethical hackers usually employ the same tools and techniques as hackers, with the important exception that they do not damage the system. They evaluate system security, update the administrators regarding any discovered vulnerabilities, and recommend procedures for patching those vulnerabilities.

The important distinction between ethical hackers and crackers is consent. Crackers attempt to gain unauthorized access to systems, while ethical hackers are always completely open and transparent about what they are doing and how they are doing it. Ethical hacking is, therefore, always legal.



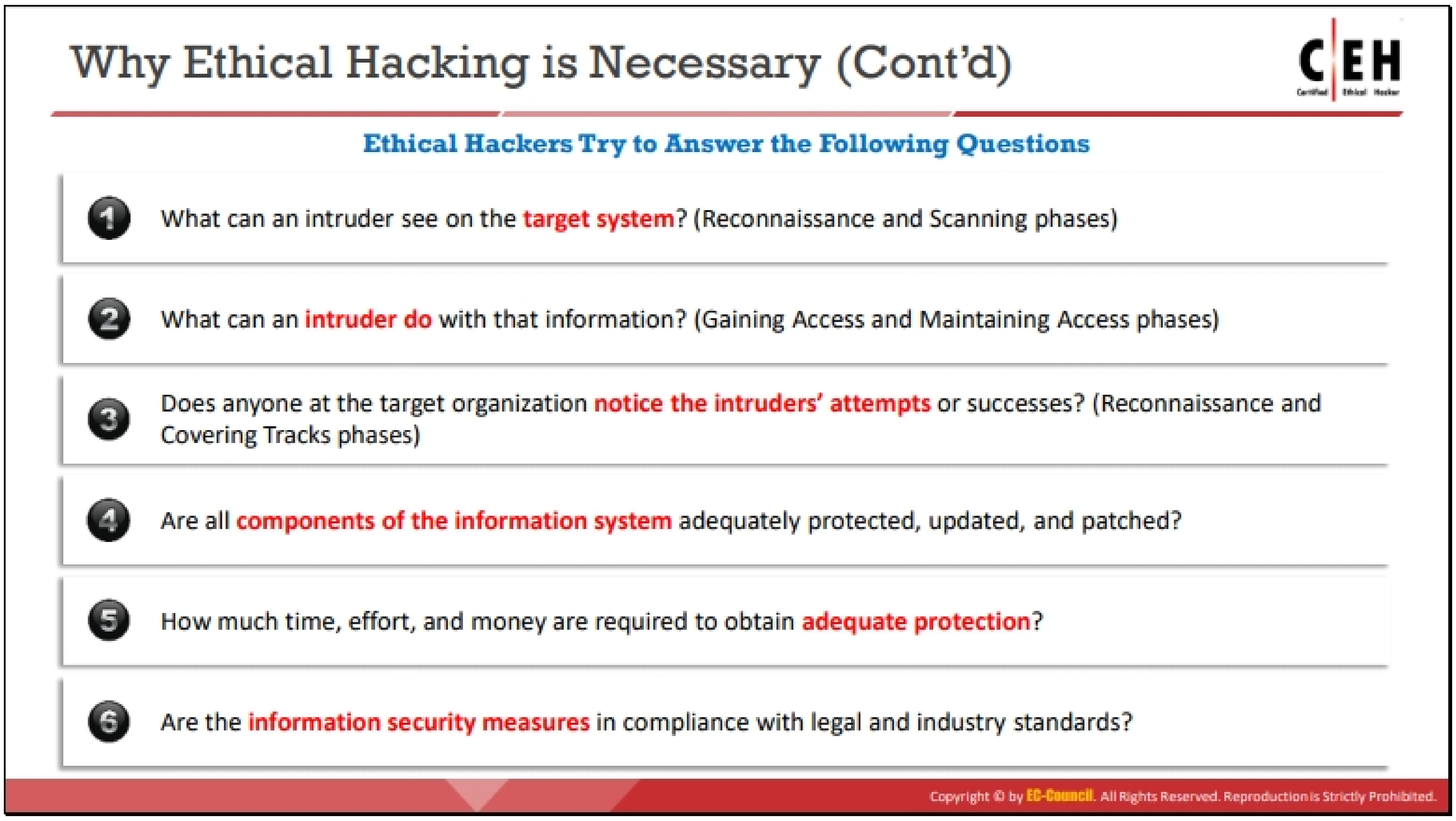
Why Ethical Hacking is Necessary

To beat a hacker, you need to think like one!

Ethical hacking is necessary as it **allows for counter attacks against malicious hackers** through anticipating the methods used to break into the system

Reasons why organizations recruit ethical hackers

- To **prevent hackers** from gaining access to the organization's information systems
- To **uncover vulnerabilities** in systems and explore their potential as a security risk
- To analyze and **strengthen an organization's security posture**, including policies, network protection infrastructure, and end-user practices
- To provide adequate preventive measures in order to **avoid security breaches**
- To help **safeguard customer data**
- To **enhance security awareness** at all levels in a business



Why Ethical Hacking is Necessary (Cont'd)

Ethical Hackers Try to Answer the Following Questions

1. What can an intruder see on the **target system**? (Reconnaissance and Scanning phases)
2. What can an **intruder do** with that information? (Gaining Access and Maintaining Access phases)
3. Does anyone at the target organization **notice the intruders' attempts** or successes? (Reconnaissance and Covering Tracks phases)
4. Are all **components of the information system** adequately protected, updated, and patched?
5. How much time, effort, and money are required to obtain **adequate protection**?
6. Are the **information security measures** in compliance with legal and industry standards?

Why Ethical Hacking is Necessary

As technology is growing at a faster pace, so is the growth in the risks associated with it. To beat a hacker, it is necessary to think like one!

Ethical hacking is necessary as it allows to counter attacks from malicious hackers by anticipating methods used by them to break into a system. Ethical hacking helps to predict various possible vulnerabilities well in advance and rectify them without incurring any kind of outside attack. As hacking involves creative thinking, vulnerability testing, and security audits alone cannot ensure that the network is secure. To achieve security, organizations must implement a "defense-in-depth" strategy by penetrating their networks to estimate and expose vulnerabilities.

Reasons why organizations recruit ethical hackers

- To prevent hackers from gaining access to the organization's information systems
- To uncover vulnerabilities in systems and explore their potential as a risk
- To analyze and strengthen an organization's security posture, including policies, network protection infrastructure, and end-user practices
- To provide adequate preventive measures in order to avoid security breaches
- To help safeguard the customer data
- To enhance security awareness at all levels in a business

An ethical hacker's evaluation of a client's information system security seeks to answer three basic questions:

1. **What can an attacker see on the target system?**

   Normal security checks by system administrators will often overlook vulnerabilities. The ethical hacker has to think about what an attacker might see during the reconnaissance and scanning phases of an attack.

2. **What can an intruder do with that information?**

   The ethical hacker must discern the intent and purpose behind attacks to determine appropriate countermeasures. During the gaining-access and maintaining-access phases of an attack, the ethical hacker needs to be one step ahead of the hacker in order to provide adequate protection.

3. **Are the attackers' attempts being noticed on the target systems?**

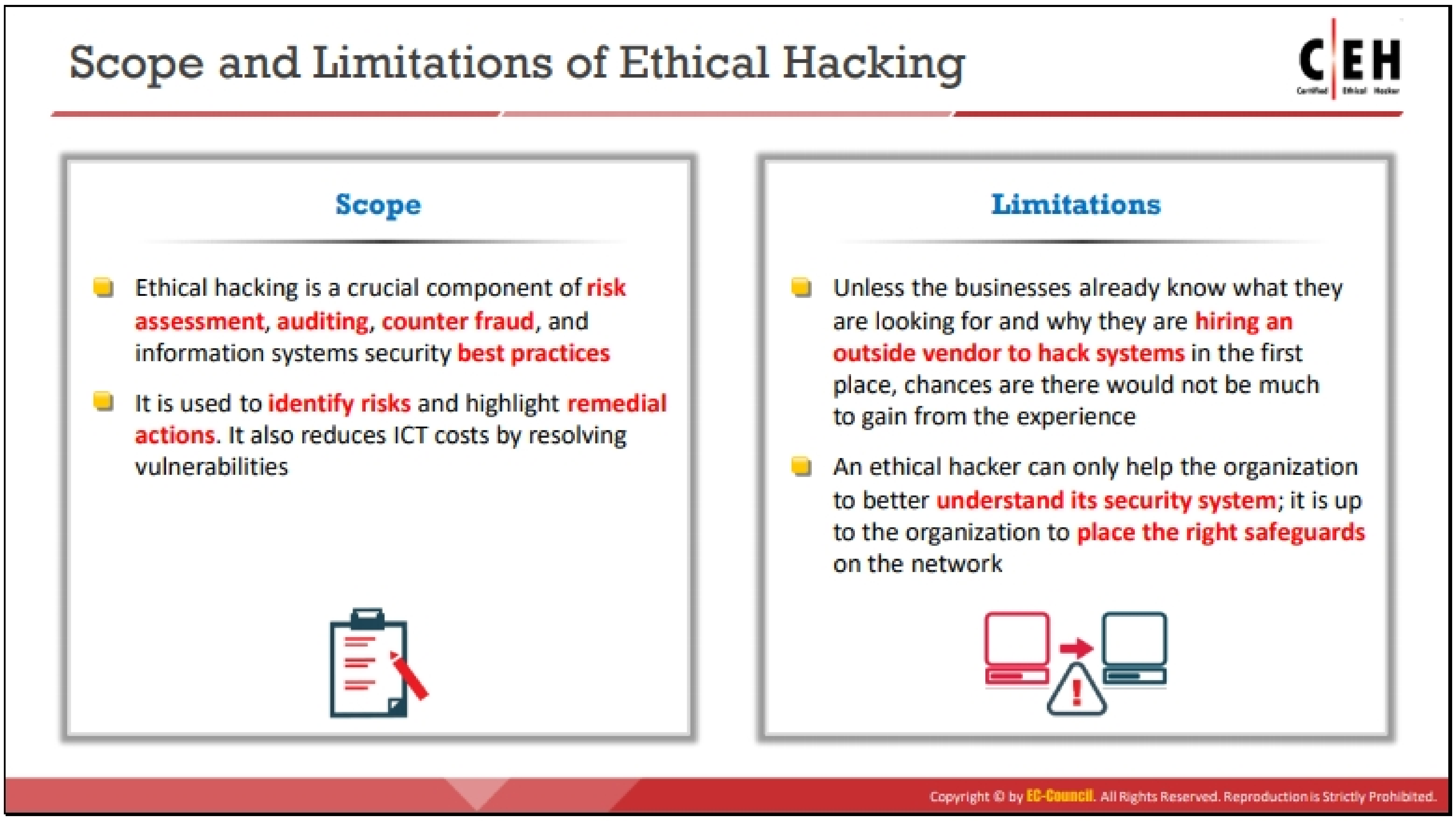
   Sometimes attackers will try to breach a system for days, weeks, or even months. Other times they will gain access but will wait before doing anything damaging. Instead, they will take the time to assess the potential use of exposed information. During the reconnaissance and covering tracks phases, the ethical hacker should notice and stop the attack.

After carrying out attacks, hackers may clear their tracks by modifying log files and creating backdoors, or by deploying trojans. Ethical hackers must investigate whether such activities have been recorded and what preventive measures have been taken. This not only provides them with an assessment of the attacker's proficiency but also gives them insight into the existing security measures of the system being evaluated. The entire process of ethical hacking and subsequent patching of discovered vulnerabilities depends on questions such as:

- What is the organization trying to protect?
- Against whom or what are they trying to protect it?

- Are all the components of the information system adequately protected, updated, and patched?
- How much time, effort, and money is the client willing to invest to gain adequate protection?
- Do the information security measures comply with industry and legal standards?

Sometimes, in order to save on resources or prevent further discovery, the client might decide to end the evaluation after the first vulnerability is found; therefore, it is important that the ethical hacker and the client work out a suitable framework for investigation beforehand. The client must be convinced of the importance of these security exercises through concise descriptions of what is happening and what is at stake. The ethical hacker must also remember to convey to the client that it is never possible to guard systems completely, but that they can always be improved.



Scope and Limitations of Ethical Hacking

C|EH Certified Ethical Hacker

Scope

- Ethical hacking is a crucial component of **risk assessment**, **auditing**, **counter fraud**, and information systems security **best practices**
- It is used to **identify risks** and highlight **remedial actions**. It also reduces ICT costs by resolving vulnerabilities

Limitations

- Unless the businesses already know what they are looking for and why they are **hiring an outside vendor to hack systems** in the first place, chances are there would not be much to gain from the experience
- An ethical hacker can only help the organization to better **understand its security system**; it is up to the organization to **place the right safeguards** on the network

Scope and Limitations of Ethical Hacking

Security experts broadly categorize computer crimes into two categories: crimes facilitated by a computer and those in which the computer is the target.

Ethical hacking is a structured and organized security assessment, usually as part of a penetration test or security audit, and is a crucial component of risk assessment, auditing, counter fraud, and information systems security best practices. It is used to identify risks and highlight remedial actions. It is also used to reduce Information and Communications Technology (ICT) costs by resolving vulnerabilities.

Ethical hackers determine the scope of the security assessment according to the client's security concerns. Many ethical hackers are members of a "Tiger Team." A tiger team works together to perform a full-scale test covering all aspects of the network, as well as physical and system intrusion.

An ethical hacker should know the penalties of unauthorized hacking into a system. No ethical hacking activities associated with a network-penetration test or security audit should begin before receiving a signed legal document giving the ethical hacker express permission to perform the hacking activities from the target organization. Ethical hackers must be judicious with their hacking skills and recognize the consequences of misusing those skills.

The ethical hacker must follow certain rules to fulfill their ethical and moral obligations. They must do the following:

- Gain authorization from the client and have a signed contract giving the tester permission to perform the test.
- Maintain confidentiality when performing the test and follow a Nondisclosure Agreement (NDA) with the client for the confidential information disclosed during the

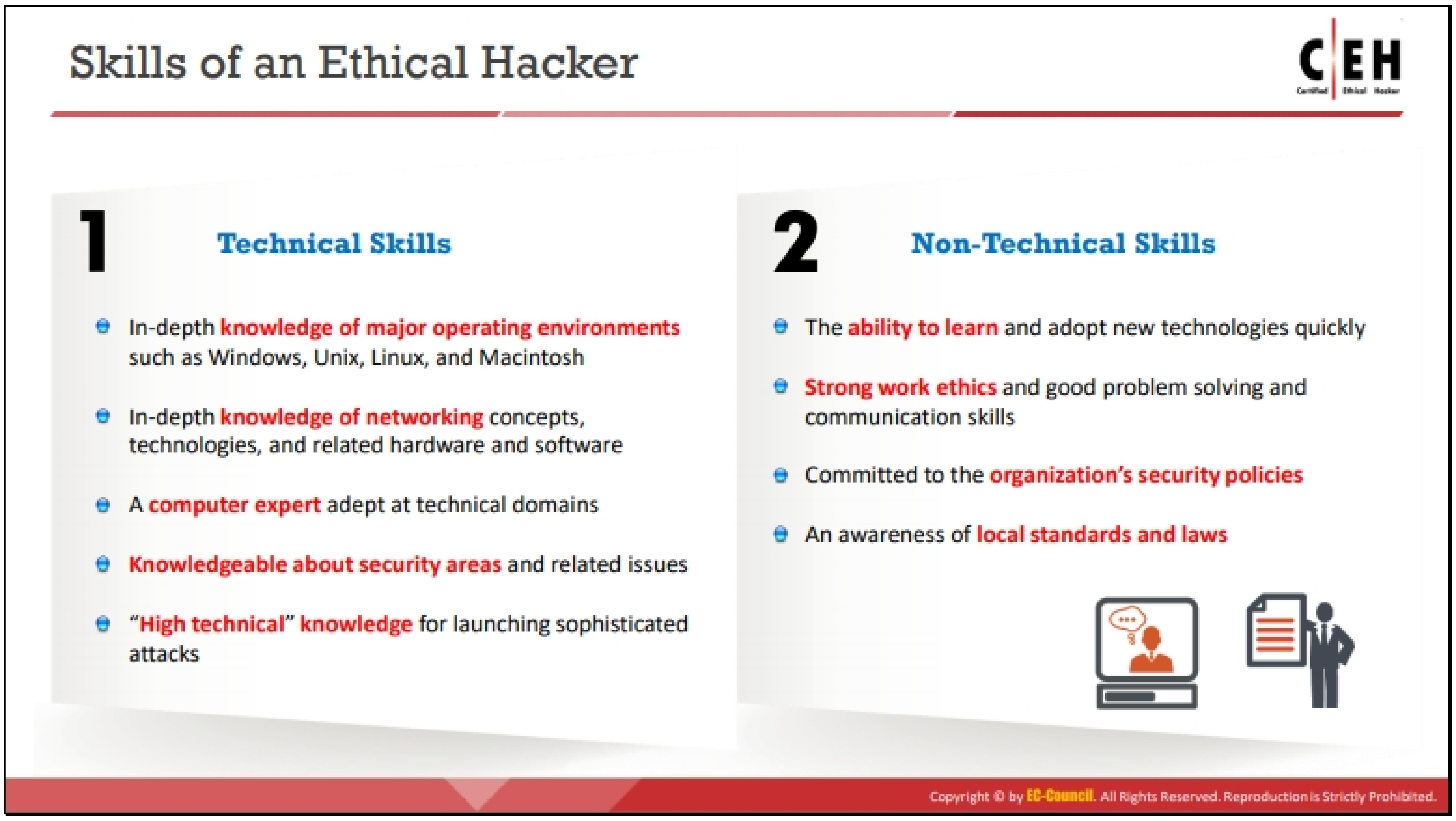
test. The information gathered might contain sensitive information, and the ethical hacker must not disclose any information about the test or the confidential company data to a third party.

- Perform the test up to but not beyond the agreed-upon limits. For example, ethical hackers should perform DoS attacks only if they have previously agreed upon this with the client. Loss of revenue, goodwill, and worse consequences could befall an organization whose servers or applications are unavailable to customers because of the testing.

The following steps provide a framework for performing a security audit of an organization, which will help in ensuring that the test is organized, efficient, and ethical:

- Talk to the client and discuss the needs to be addressed during the testing
- Prepare and sign NDA documents with the client
- Organize an ethical hacking team and prepare the schedule for testing
- Conduct the test
- Analyze the results of the testing and prepare a report
- Present the report findings to the client

However, there are limitations too. Unless the businesses first know what they are looking for and why they are hiring an outside vendor to hack their systems in the first place, chances are there would not be much to gain from experience. An ethical hacker, thus, can only help the organization to better understand its security system. It is up to the organization to place the right safeguards on the network.



Skills of an Ethical Hacker

1 Technical Skills

- In-depth **knowledge of major operating environments** such as Windows, Unix, Linux, and Macintosh
- In-depth **knowledge of networking** concepts, technologies, and related hardware and software
- A **computer expert** adept at technical domains
- **Knowledgeable about security areas** and related issues
- "**High technical**" **knowledge** for launching sophisticated attacks

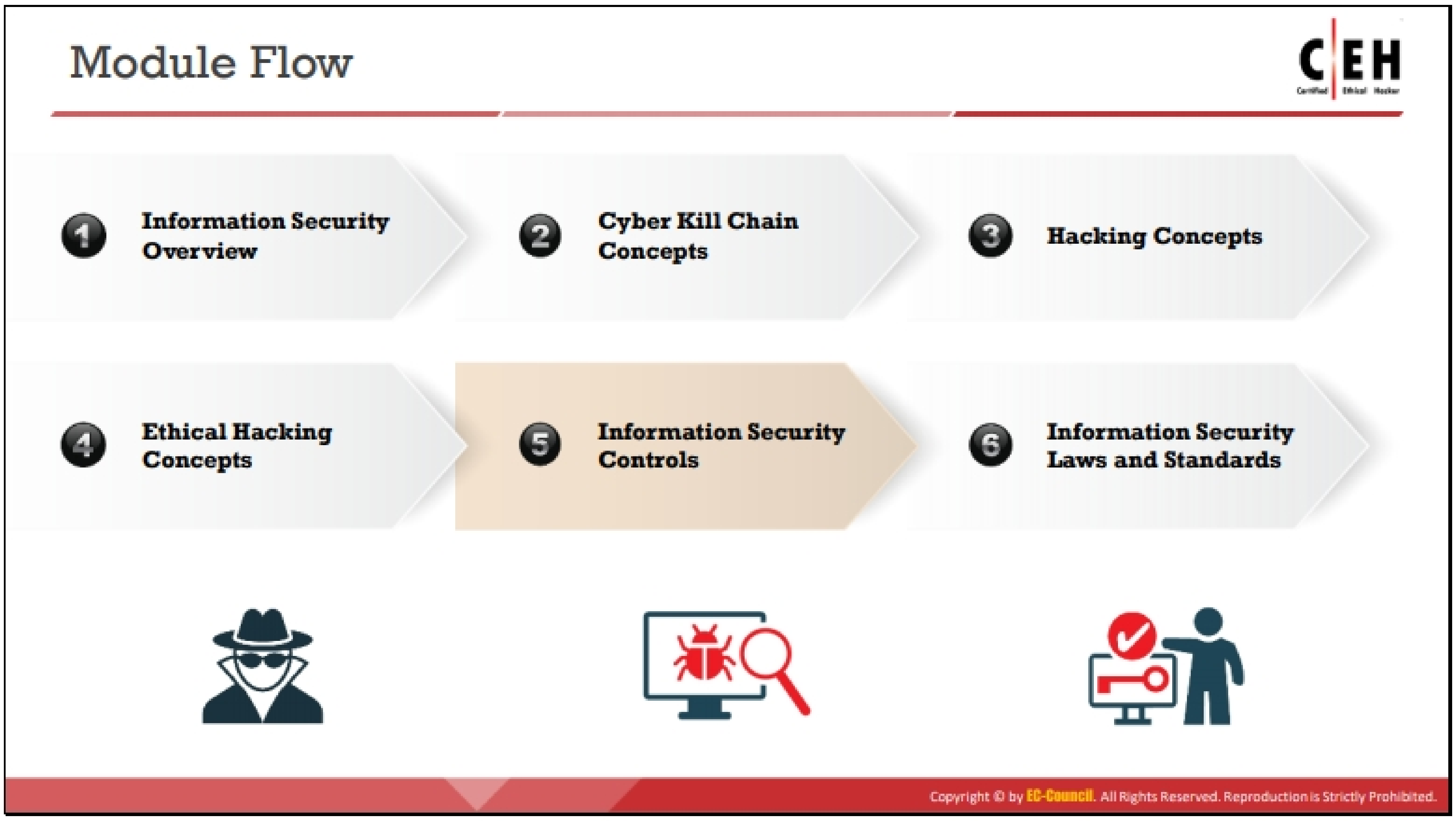
2 Non-Technical Skills

- The **ability to learn** and adopt new technologies quickly
- **Strong work ethics** and good problem solving and communication skills
- Committed to the **organization's security policies**
- An awareness of **local standards and laws**

Skills of an Ethical Hacker

It is essential for an ethical hacker to acquire the knowledge and skills to become an expert hacker and to use this knowledge in a lawful manner. The technical and non-technical skills to be a good ethical hacker are discussed below:

- **Technical Skills**
  - In-depth knowledge of major operating environments, such as Windows, Unix, Linux, and Macintosh
  - In-depth knowledge of networking concepts, technologies, and related hardware and software
  - A computer expert adept at technical domains
  - The knowledge of security areas and related issues
  - High technical knowledge of how to launch sophisticated attacks
- **Non-Technical Skills**
  - The ability to quickly learn and adapt new technologies
  - A strong work ethic and good problem solving and communication skills
  - Commitment to an organization's security policies
  - An awareness of local standards and laws



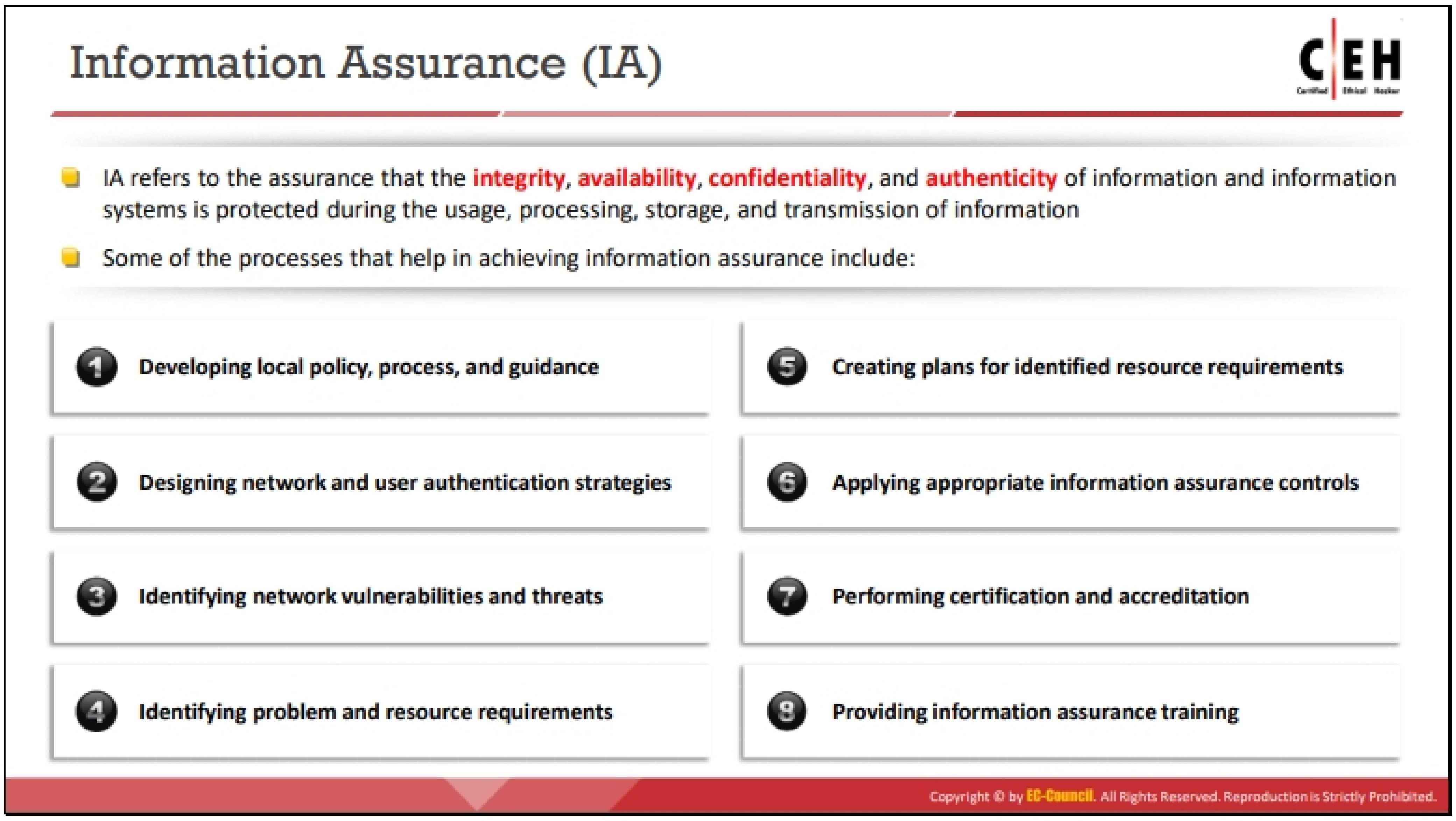
Module Flow

1. Information Security Overview
2. Cyber Kill Chain Concepts
3. Hacking Concepts
4. Ethical Hacking Concepts
5. Information Security Controls
6. Information Security Laws and Standards

Information Security Controls

Information security controls prevent the occurrence of unwanted events and reduce risk to the organization's information assets. The basic security concepts critical to information on the Internet are confidentiality, integrity, and availability; the concepts related to the persons accessing the information are authentication, authorization, and non-repudiation. Information is the greatest asset of an organization. It must be secured using various policies, creating awareness, employing security mechanisms, or by other means.

This section deals with Information Assurance (IA), defense-in-depth, risk management, cyber threat intelligence, threat modeling, incident management, and AI and ML concepts.



Information Assurance (IA)

- IA refers to the assurance that the **integrity**, **availability**, **confidentiality**, and **authenticity** of information and information systems is protected during the usage, processing, storage, and transmission of information
- Some of the processes that help in achieving information assurance include:

1. **Developing local policy, process, and guidance**
2. **Designing network and user authentication strategies**
3. **Identifying network vulnerabilities and threats**
4. **Identifying problem and resource requirements**
5. **Creating plans for identified resource requirements**
6. **Applying appropriate information assurance controls**
7. **Performing certification and accreditation**
8. **Providing information assurance training**

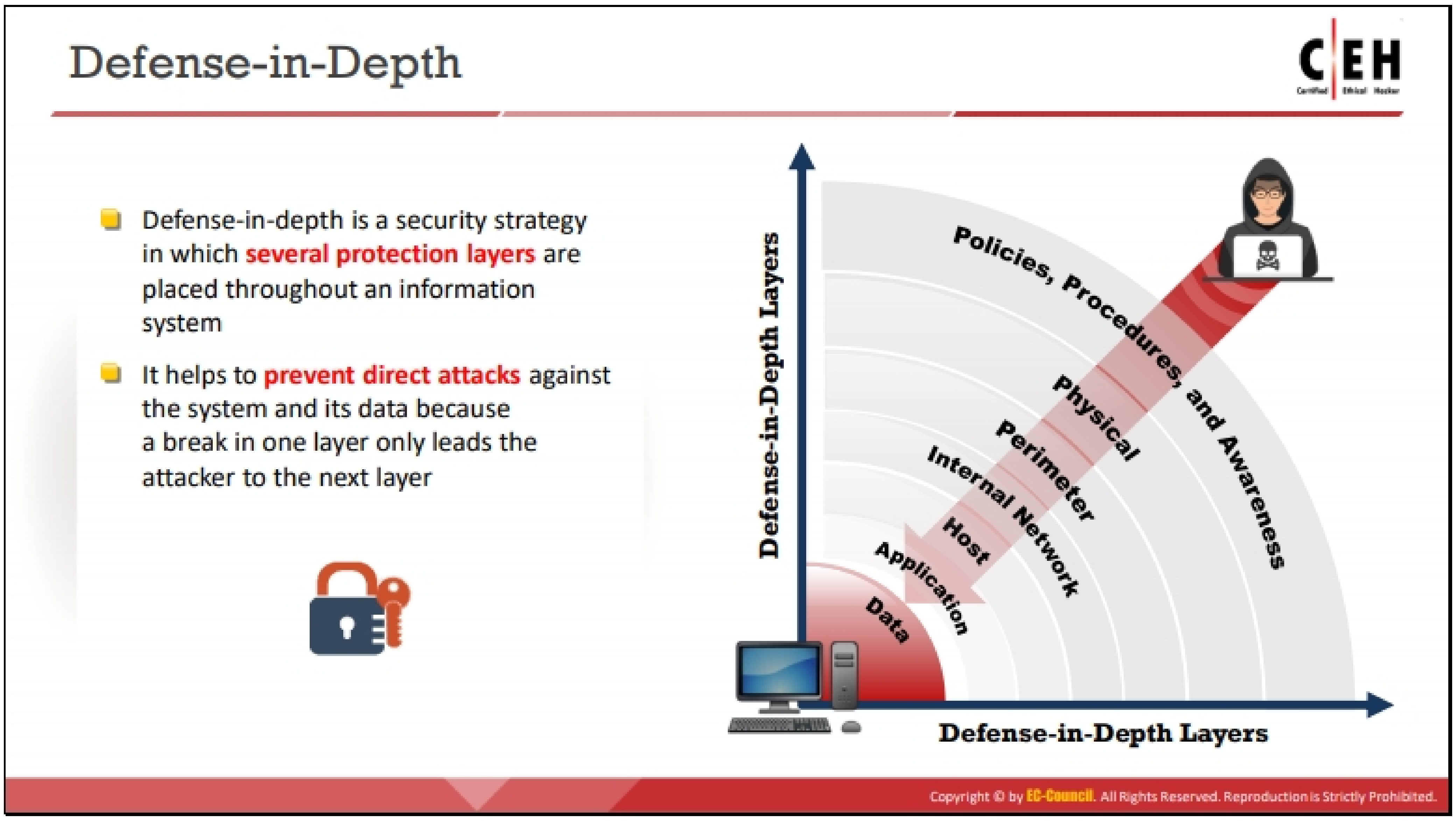
Information Assurance (IA)

IA refers to the assurance of the integrity, availability, confidentiality, and authenticity of information and information systems during the usage, processing, storage, and transmission of information. Security experts accomplish information assurance with the help of physical, technical, and administrative controls. Information Assurance and Information Risk Management (IRM) ensure that only authorized personnel access and use information. This helps in achieving information security and business continuity.

Some of the processes that help in achieving information assurance include:

- Developing local policy, process, and guidance in such a way to maintain the information systems at an optimum security level
- Designing network and user authentication strategy—Designing a secure network ensures the privacy of user records and other information on the network. Implementing an effective user authentication strategy secures the information system's data
- Identifying network vulnerabilities and threats—Vulnerability assessments outline the security posture of the network. Performing vulnerability assessments in search of network vulnerabilities and threats help to take the proper measures to overcome them
- Identifying problems and resource requirements
- Creating a plan for identified resource requirements
- Applying appropriate information assurance controls
- Performing the Certification and Accreditation (C&A) process of information systems helps to trace vulnerabilities, and implement safety measures to nullify them

- Providing information assurance training to all personnel in federal and private organizations brings among them an awareness of information technology



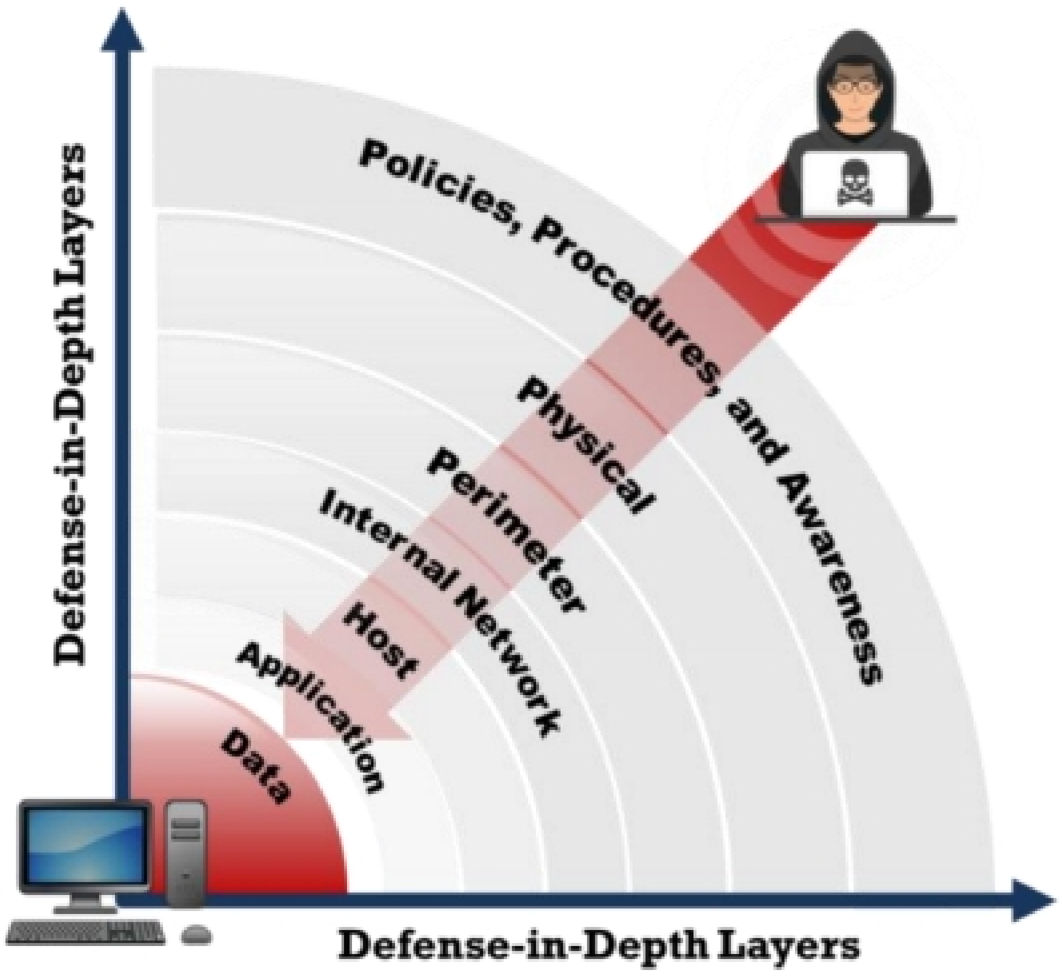
Defense-in-Depth

- Defense-in-depth is a security strategy in which **several protection layers** are placed throughout an information system
- It helps to **prevent direct attacks** against the system and its data because a break in one layer only leads the attacker to the next layer

Defense-in-Depth Layers
Policies, Procedures, and Awareness
Physical
Perimeter
Internal Network
Host
Application
Data
Defense-in-Depth Layers

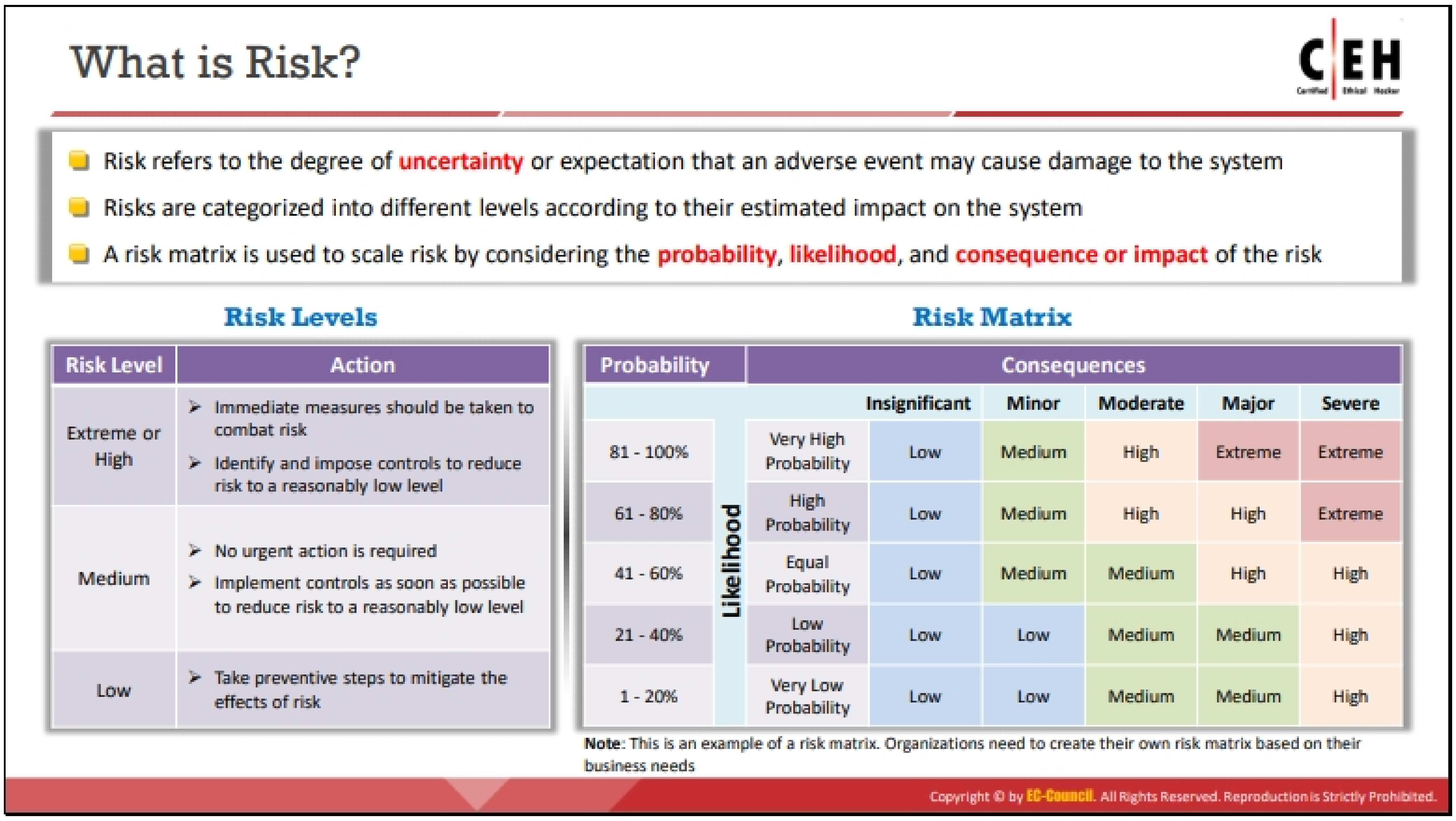
Defense-in-Depth

Defense-in-depth is a security strategy in which security professionals use several protection layers throughout an information system. This strategy uses the military principle that it is more difficult for an enemy to defeat a complex and multi-layered defense system than to penetrate a single barrier. Defense-in-depth helps to prevent direct attacks against an information system and its data because a break in one layer only leads the attacker to the next layer. If a hacker gains access to a system, defense-in-depth minimizes any adverse impact and gives administrators and engineers time to deploy new or updated countermeasures to prevent a recurrence of the intrusion.



Defense-in-Depth Layers
Policies, Procedures, and Awareness
Physical
Perimeter
Internal Network
Host
Application
Data
Defense-in-Depth Layers

Figure 1.3: Defense in Depth



What is Risk?

- Risk refers to the degree of **uncertainty** or expectation that an adverse event may cause damage to the system
- Risks are categorized into different levels according to their estimated impact on the system
- A risk matrix is used to scale risk by considering the **probability**, **likelihood**, and **consequence or impact** of the risk

Risk Levels

Risk Level	Action
Extreme or High	➢ Immediate measures should be taken to combat risk ➢ Identify and impose controls to reduce risk to a reasonably low level
Medium	➢ No urgent action is required ➢ Implement controls as soon as possible to reduce risk to a reasonably low level
Low	➢ Take preventive steps to mitigate the effects of risk

Risk Matrix

Probability		Consequences				
	Likelihood	Insignificant	Minor	Moderate	Major	Severe
81 - 100%	Very High Probability	Low	Medium	High	Extreme	Extreme
61 - 80%	High Probability	Low	Medium	High	High	Extreme
41 - 60%	Equal Probability	Low	Medium	Medium	High	High
21 - 40%	Low Probability	Low	Low	Medium	Medium	High
1 - 20%	Very Low Probability	Low	Low	Medium	Medium	High

Note: This is an example of a risk matrix. Organizations need to create their own risk matrix based on their business needs

What is Risk?

Risk refers to the degree of uncertainty or expectation of potential damage that an adverse event may cause to the system or its resources, under specified conditions. Alternatively, risk can also be:

- The probability of the occurrence of a threat or an event that will damage, cause loss to, or have other negative impacts on the organization, either from internal or external liabilities.
- The possibility of a threat acting upon an internal or external vulnerability and causing harm to a resource.
- The product of the likelihood that an event will occur and the impact that the event might have on an information technology asset.

The relation between Risk, Threats, Vulnerabilities, and Impact is as follows:

RISK = Threats x Vulnerabilities x Impact

The impact of an event on an information asset is the product of vulnerability in the asset and the asset's value to its stakeholders. IT risk can be expanded to

RISK = Threat × Vulnerability × Asset Value

In fact, the risk is the combination of the following two factors:

- The probability of the occurrence of an adverse event
- The consequence of the adverse event

Risk Level

Risk level is an assessment of the resulted impact on the network. Various methods exist to differentiate the risk levels depending on the risk frequency and severity. One of the common methods used to classify risks is to develop a two-dimensional matrix.

Working out the frequency or probability of an incident happening (likelihood) and its possible consequences is necessary to analyze risks. This is referred to as the level of risk. Risk can be represented and calculated using the following formula:

Level of Risk = Consequence x Likelihood

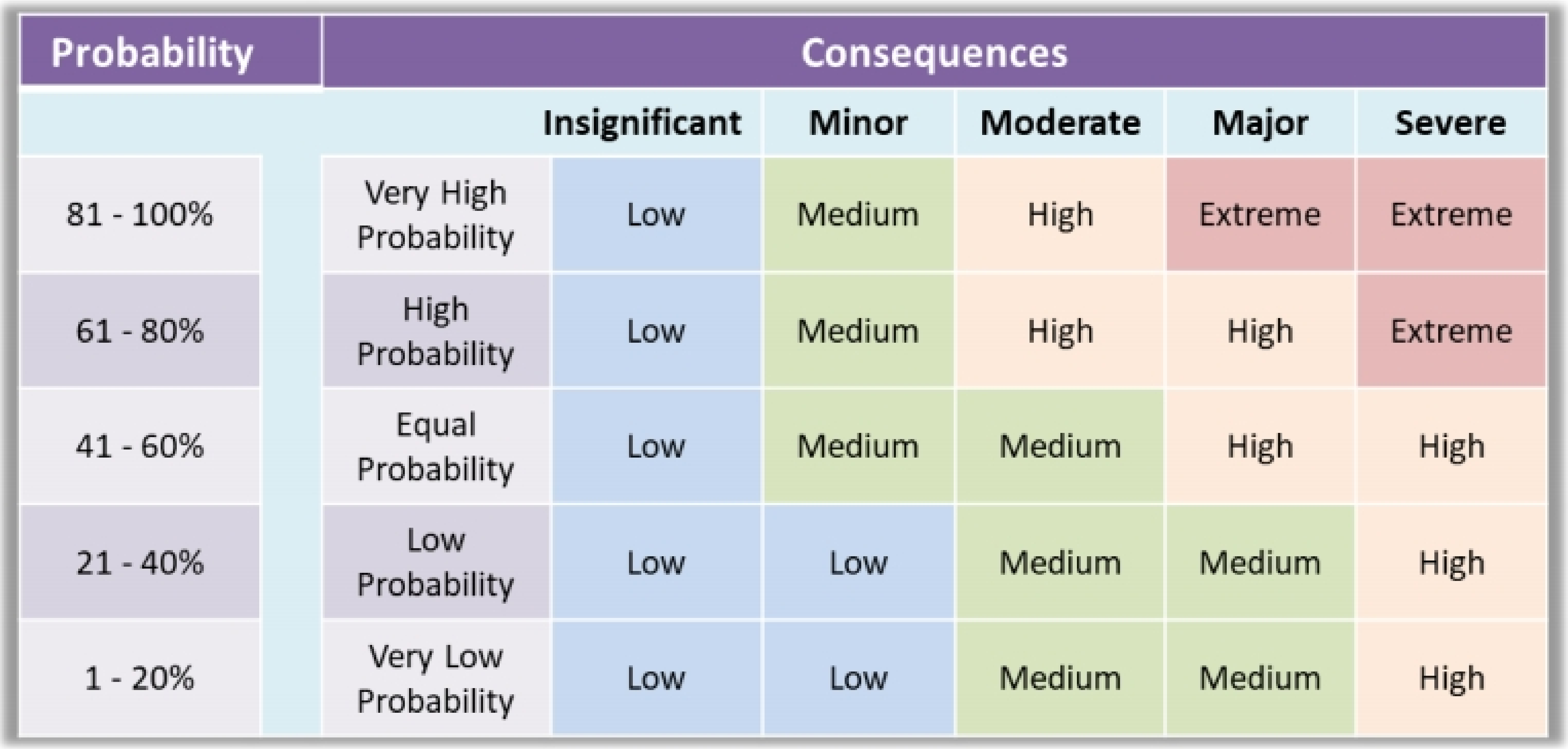
Risks are categorized into different levels according to their estimated impact on the system. Primarily, there are four risk levels, which include extreme, high, medium, and low levels. Remember that control measures may decrease the level of a risk, but do not always entirely eliminate the risk.

Risk Level	Consequence	Action
Extreme or High	Serious or Imminent danger	➢ Immediate measures are required to combat the risk ➢ Identify and impose controls to reduce the risk to a reasonably low level
Medium	Moderate danger	➢ Immediate action is not required, but action should be implement quickly ➢ Implement controls as soon as possible to reduce the risk to a reasonably low level
Low	Negligible danger	➢ Take preventive steps to mitigate the effects of risk

Table 1.1: Risk Levels

Risk Matrix

The risk matrix scales the risk occurrence or likelihood probability, along with its consequences or impact. It is the graphical representation of risk severity and the extent to which the controls can or will mitigate it. The Risk matrix is one of the simplest processes to use for increased visibility of risk; it contributes to the management's decision-making capability. The risk matrix defines various levels of risk and categorizes them as the product of negative probability and negative severity. Although there are many standard risk matrices, individual organizations must create their own.



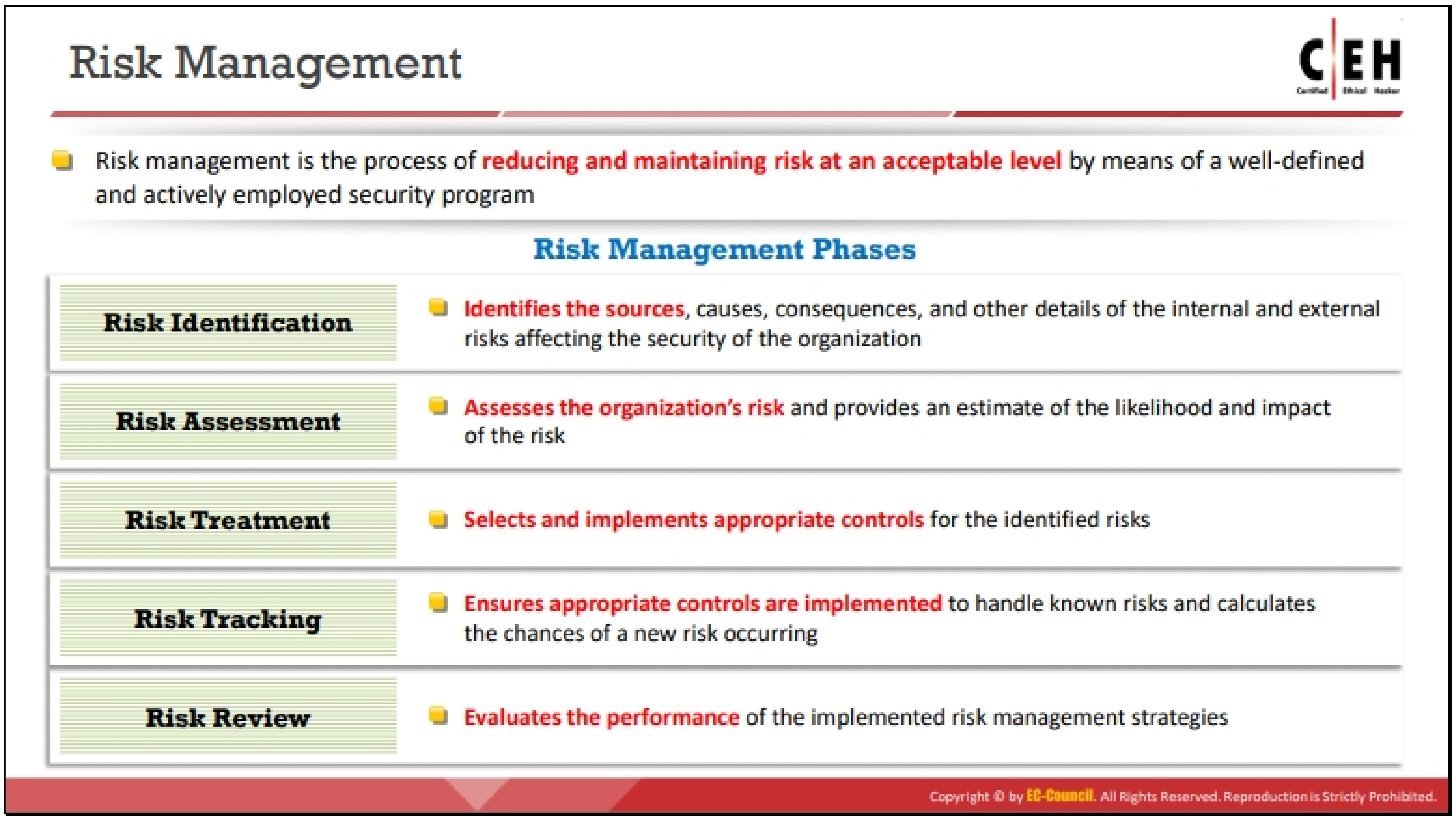
Probability	Consequences					
		Insignificant	**Minor**	**Moderate**	**Major**	**Severe**
81 - 100%	Very High Probability	Low	Medium	High	Extreme	Extreme
61 - 80%	High Probability	Low	Medium	High	High	Extreme
41 - 60%	Equal Probability	Low	Medium	Medium	High	High
21 - 40%	Low Probability	Low	Low	Medium	Medium	High
1 - 20%	Very Low Probability	Low	Low	Medium	Medium	High

Table 1.2: Risk Matrix

The above table is the graphical representation of a risk matrix, which is used to visualize and compare risks. It differentiates the two levels of risk and is a simple way of analyzing them.

- Likelihood: The chance of the risk occurring
- Consequence: The severity of a risk event that occurs

Note: This is an example of a risk matrix. Organizations must create individual risk matrices based on their business needs.



Risk Management

- Risk management is the process of **reducing and maintaining risk at an acceptable level** by means of a well-defined and actively employed security program

Risk Management Phases

Risk Identification	**Identifies the sources**, causes, consequences, and other details of the internal and external risks affecting the security of the organization
Risk Assessment	**Assesses the organization's risk** and provides an estimate of the likelihood and impact of the risk
Risk Treatment	**Selects and implements appropriate controls** for the identified risks
Risk Tracking	**Ensures appropriate controls are implemented** to handle known risks and calculates the chances of a new risk occurring
Risk Review	**Evaluates the performance** of the implemented risk management strategies

Risk Management

Risk management is the process of identifying, assessing, responding to, and implementing the activities that control how the organization manages the potential effects of risk. It has a prominent place throughout the security life cycle and is a continuous and ever-increasing complex process. The types of risks vary from organization to organization, but the act of preparing a risk management plan is common to all organizations.

Risk Management Objectives

- Identify potential risks—this is the main objective of risk management
- Identify the impact of risks and help the organization develop better risk management strategies and plans
- Prioritize the risks, depending on the impact or severity of the risk, and use established risk management methods, tools, and techniques to assist in this task
- Understand and analyze the risks and report identified risk events.
- Control the risk and mitigate its effect.
- Create awareness among the security staff and develop strategies and plans for lasting risk management strategies.

Risk management is a continuous process performed by achieving goals at every phase. It helps reduce and maintain risk at an acceptable level utilizing a well-defined and actively employed security program. This process is applied in all stages of the organization, for example, to specific network locations in both strategic and operational contexts.

The four key steps commonly termed as risk management phases are:

- Risk Identification
- Risk Assessment
- Risk Treatment
- Risk Tracking and Review

Every organization should follow the above steps while performing the risk management process.

- **Risk Identification**

  The initial step of the risk management plan. Its main aim is to identify the risks—including the sources, causes, and consequences of the internal and external risks affecting the security of the organization before they cause harm. The risk identification process depends on the skill set of the people, and it differs from one organization to another.

- **Risk Assessment**

  This phase assesses the organization's risks and estimates the likelihood and impact of those risks. Risk assessment is an ongoing iterative process that assigns priorities for risk mitigation and implementation plans, which in turn help to determine the quantitative and qualitative value of risk. Every organization should adopt a risk evaluation process in order to detect, prioritize, and remove risks.

  The risk assessment determines the kind of risks present, their likelihood and severity, and the priorities and plans for risk control. Organizations perform a risk assessment when they identify a hazard but are not able to control it immediately. A risk assessment is followed by a regular update of all information facilities.

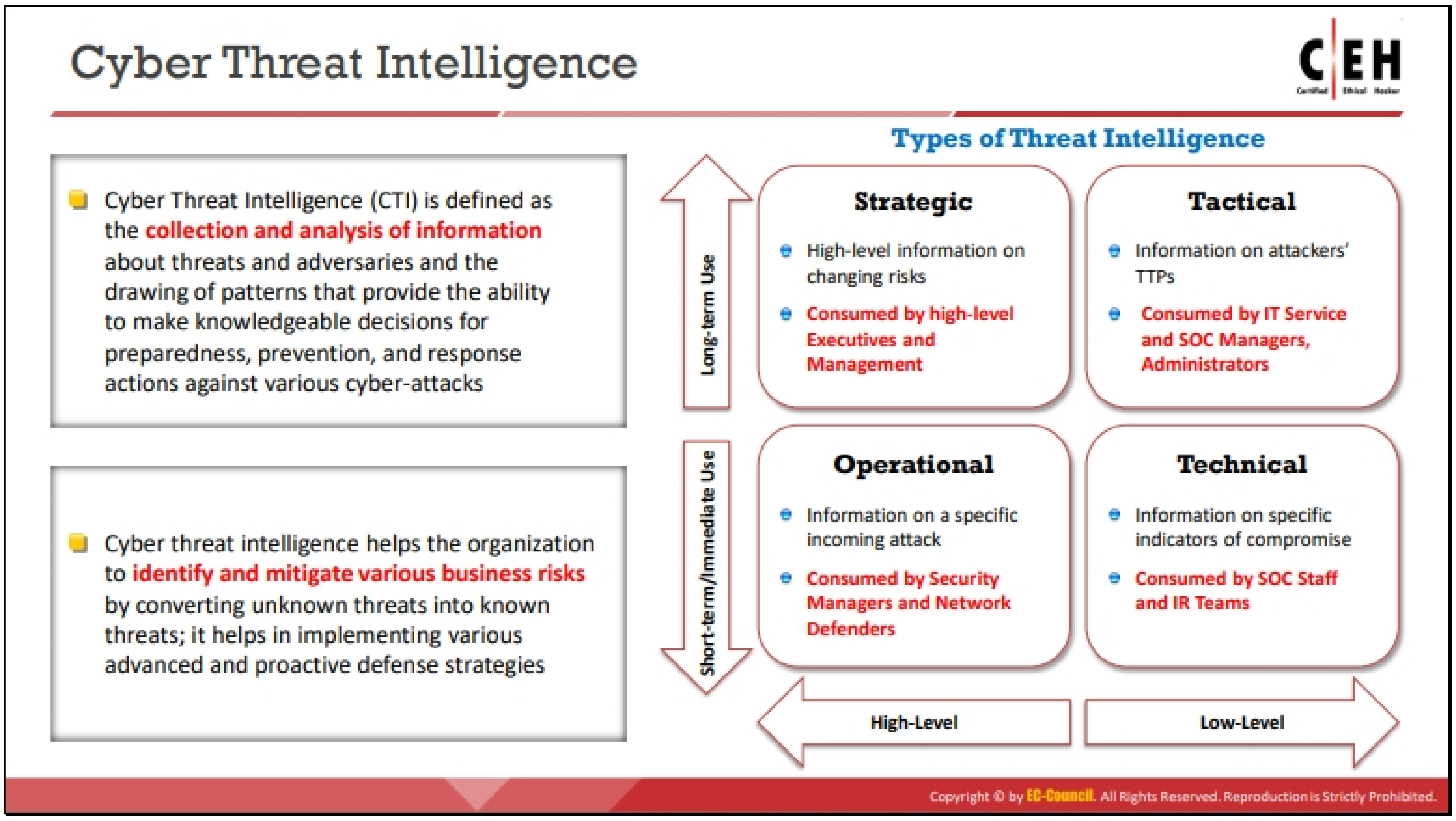
- **Risk Treatment**

  Risk treatment is the process of selecting and implementing appropriate controls on the identified risks in order to modify them. The risk treatment method addresses and treats the risks according to their severity level. Decisions made in this phase are based on the results of a risk assessment. The purpose of this step is to identify treatments for the risks that fall outside the department's risk tolerance and provide an understanding of the level of risk with controls and treatments. It identifies the priority order in which individual risks should be treated, monitored, and reviewed. The following information is needed before treating the risk:

  - The appropriate method of treatment
  - The people responsible for the treatment
  - The costs involved
  - The benefits of treatment
  - The likelihood of success
  - Ways to measure and assess the treatment

- **Risk Tracking and Review**

  An effective risk management plan requires a tracking and review structure to ensure effective identification and assessment of the risks as well as the use of appropriate controls and responses. The tracking and review process should determine the measures and procedures adopted and ensure that the information gathered to perform the assessment was appropriate. The review phase evaluates the performance of the implemented risk management strategies. Performing regular inspections of policies and standards, as well as regularly reviewing them, helps to identify the opportunities for improvement. Further, the monitoring process ensures that there are appropriate controls in place for the organization’s activities and that all procedures are understood and followed.



Cyber Threat Intelligence

- Cyber Threat Intelligence (CTI) is defined as the **collection and analysis of information** about threats and adversaries and the drawing of patterns that provide the ability to make knowledgeable decisions for preparedness, prevention, and response actions against various cyber-attacks

- Cyber threat intelligence helps the organization to **identify and mitigate various business risks** by converting unknown threats into known threats; it helps in implementing various advanced and proactive defense strategies

Types of Threat Intelligence

Strategic
- High-level information on changing risks
- **Consumed by high-level Executives and Management**

Tactical
- Information on attackers' TTPs
- **Consumed by IT Service and SOC Managers, Administrators**

Operational
- Information on a specific incoming attack
- **Consumed by Security Managers and Network Defenders**

Technical
- Information on specific indicators of compromise
- **Consumed by SOC Staff and IR Teams**

Cyber Threat Intelligence

According to the Oxford dictionary, a threat is defined as "the possibility of a malicious attempt to damage or disrupt a computer network or system." A threat is a potential occurrence of an undesired event that can eventually damage and interrupt the operational and functional activities of an organization. A threat can affect the integrity and availability factors of an organization. The impact of threats is very great and may affect the state of the physical IT assets in an organization. The existence of threats may be accidental, intentional, or due to the impact of some action.

Cyber threat intelligence, usually known as CTI, is the collection and analysis of information about threats and adversaries and the drawing up of patterns that provide an ability to make knowledgeable decisions for preparedness, prevention, and response actions against various cyberattacks. It is the process of recognizing or discovering any "unknown threats" that an organization may face so that necessary defense mechanisms can be applied to avoid such occurrences. It involves collecting, researching, and analyzing trends and technical developments in the field of cyber threats (including cybercrime, hacktivism, and espionage). Any knowledge about threats that results in an organization's planning and decision-making to handle it is a piece of threat Intelligence. The main aim of CTI is to make the organization aware of existing or emerging threats and prepare them to develop a proactive cybersecurity posture in advance of exploitation. This process, where unknown threats are converted into possibly known ones, helps to anticipate the attack before it can happen, and ultimately results in a better and more secure system. Thus, threat Intelligence is useful in achieving secure data sharing and global transactions among organizations.

Threat intelligence processes can be used to identify the risk factors that are responsible for malware attacks, SQL injections, web application attacks, data leaks, phishing, denial-of-service attack, and other attacks. Such risks, after being filtered out, can be put on a checklist and handled appropriately. Threat intelligence is beneficial for an organization to handle cyber threats with effective planning and execution. Along with a thorough analysis of the threat, CTI also strengthens the organization's defense system, creates awareness about impending risks, and aids in responding against such risks.

Types of Threat Intelligence

Threat intelligence is contextual information that describes threats and guides organizations in making various business decisions. It is extracted from a huge collection of sources and information. It provides operational insight by looking outside the organization and issuing alerts on evolving threats to the organization. For the better management of information that is collected from different sources, it is important to subdivide threat intelligence into different types. This subdivision is performed based on the consumers and goals of the intelligence. From the perspective of consumption, threat intelligence is divided into four different types. They are, namely, strategic, tactical, operational, and technical threat intelligence. These four types differ in terms of data collection, data analysis, and intelligence consumption.

- **Strategic Threat Intelligence**

  Strategic threat intelligence provides high-level information regarding cybersecurity posture, threats, details about the financial impact of various cyber activities, attack trends, and the impact of high-level business decisions. This information is consumed by the high-level executives and management of the organization, such as IT management and CISO. It helps the management to identify current cyber risks, unknown future risks, threat groups, and attribution of breaches. The intelligence obtained provides a risk-based view that mainly focuses on high-level concepts of risks and their probability. It mainly deals with long-term issues and provides real-time alerts for threats to the organization's critical assets, such as IT infrastructure, employees, customers, and applications. This intelligence is used by the management to make strategic business decisions and to analyze their effect. Based on the analysis, the management can allocate sufficient budget and staff to protect critical IT assets and business processes.

  Strategic threat intelligence is generally in the form of a report that mainly focuses on high-level business strategies. Since the characteristic of strategic threat intelligence is preeminent, the data collection also relates to high-level sources and requires highly skilled professionals to extract information. This intelligence is collected from sources such as OSINT, CTI vendors, and ISAOs and ISACs.

  The strategic threat intelligence helps organizations identify any similar past incidents, their intentions, and any attributes that might identify the attacking adversaries, why the organization is within the scope of the attack, major attack trends, and how to reduce the risk level.

  Generally, strategic threat intelligence includes the following information:

  - The financial impact of cyber activity
  - Attribution for intrusions and data breaches

  - Threat actors and attack trends
  - The threat landscape for various industry sectors
  - Statistical information on data breaches, data theft, and malware
  - Geopolitical conflicts involving various cyberattacks
  - Information on how adversary TTPs change over time
  - Industry sectors that might impact due to high-level business decisions

- **Tactical Threat Intelligence**

  Tactical threat intelligence plays a major role in protecting the resources of the organization. It provides information related to the TTPs used by threat actors (attackers) to perform attacks. Tactical threat intelligence is consumed by cybersecurity professionals such as IT service managers, security operations managers, network operations center (NOC) staff, administrators, and architects. It helps the cybersecurity professionals understand how the adversaries are expected to perform their attack on the organization, identify the information leakage from the organization, and assess the technical capabilities and goals of the attackers along with the attack vectors. Using tactical threat intelligence, security personnel develop detection and mitigation strategies beforehand through procedures such as updating security products with identified indicators and patching vulnerable systems.

  The collection sources for tactical threat intelligence include campaign reports, malware, incident reports, attack group reports, and human intelligence, among other information. This intelligence is generally obtained by reading white or technical papers, communicating with other organizations, or purchasing intelligence from third parties. It includes highly technical information on topics such as malware, campaigns, techniques, and tools in the form of forensic reports.

  Tactical threat intelligence provides day-to-day operational support by helping analysts assess various security incidents related to events, investigations, and other activities. It also guides the high-level executives of the organizations in making strategic business decisions.

- **Operational Threat Intelligence**

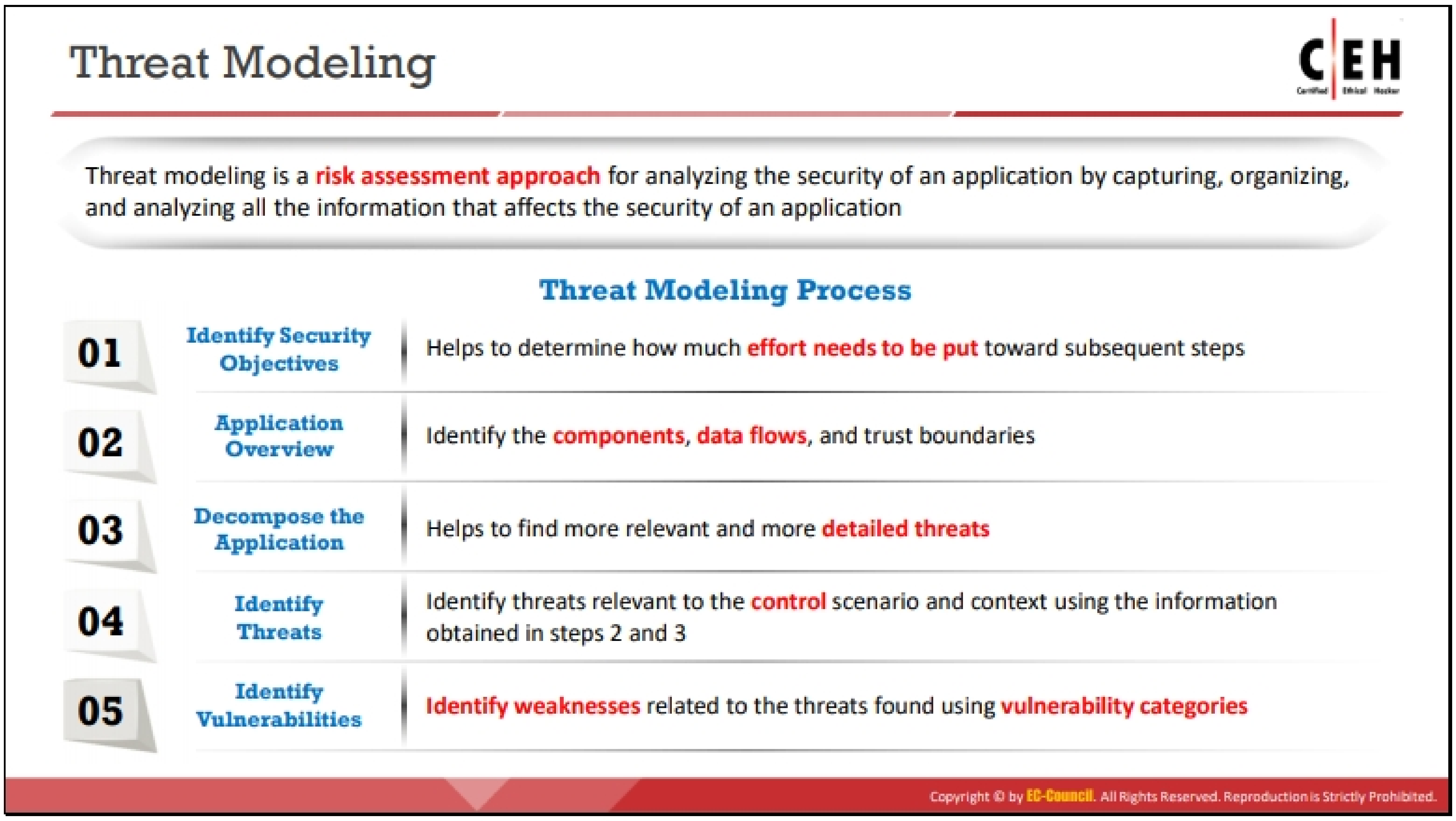
  Operational threat intelligence provides information about specific threats against the organization. It provides contextual information about security events and incidents that help defenders disclose potential risks, provide greater insight into attacker methodologies, identify past malicious activities, and perform investigations on malicious activity in a more efficient way. It is consumed by security managers or heads of incident response, network defenders, security forensics, and fraud detection teams. It helps organizations to understand the possible threat actors and their intention, capability, and opportunity to attack vulnerable IT assets and the impact of a successful attack. In many cases, only government organizations can collect this type of intelligence. However, doing so helps IR and forensic teams to deploy security assets to identify and stop upcoming attacks, improve early-stage attack detecting capability, and reduce an attack's damage to IT assets.

Operational threat intelligence is generally collected from sources such as humans, social media, and chat rooms; it may and also be collected from the real-world activities and events that result in cyberattacks. Operational threat intelligence is obtained by analyzing human behavior, threat groups, and by similar means. This information helps to predict future attacks and thus enhances incident response plans and mitigation strategies. Operational threat intelligence generally appears as a report that contains identified malicious activities, recommended courses of action, and warnings of emerging attacks.

- **Technical Threat Intelligence**

  Technical threat intelligence provides information about resources an attacker uses to perform an attack; this includes command and control channels, tools, and other items. It has a shorter lifespan compared to tactical threat intelligence and mainly focuses on a specific IoC. It provides rapid distribution and response to threats. For example, a piece of malware used to perform an attack is tactical threat intelligence, whereas the details related to the specific implementation of the malware come under technical threat intelligence. Other examples of technical threat intelligence include the specific IP addresses and domains used by malicious endpoints, phishing email headers, and hash checksums of malware, among others. Technical threat intelligence is consumed by SOC staff and IR teams.

  The indicators of technical threat intelligence are collected from active campaigns, attacks that are performed on other organizations, or data feeds provided by external third parties. These indicators are generally collected as part of investigations of attacks performed on various organizations. This information helps security professionals add the identified indicators to the defensive systems such as IDS and IPS, firewalls, and endpoint security systems, thereby enhancing the detection mechanisms used to identify the attacks at an early stage. It also helps them identify malicious traffic and IP addresses suspected of spreading malware and spam emails. This intelligence is directly fed into the security devices in digital format to block and identify inbound and outbound malicious traffic entering the organization's network.



Threat Modeling

Threat modeling is a **risk assessment approach** for analyzing the security of an application by capturing, organizing, and analyzing all the information that affects the security of an application

Threat Modeling Process

01	**Identify Security Objectives**	Helps to determine how much **effort needs to be put** toward subsequent steps
02	**Application Overview**	Identify the **components**, **data flows**, and trust boundaries
03	**Decompose the Application**	Helps to find more relevant and more **detailed threats**
04	**Identify Threats**	Identify threats relevant to the **control** scenario and context using the information obtained in steps 2 and 3
05	**Identify Vulnerabilities**	**Identify weaknesses** related to the threats found using **vulnerability categories**

Threat Modeling

Threat modeling is a risk assessment approach for analyzing the security of an application by capturing, organizing, and analyzing all the information that affects it. The threat model consists of three major building blocks: understanding the adversary's perspective, characterizing the security of the system, and determining threats. Every application should have a developed and documented threat model that should be revisited as the application evolves and development progresses.

Threat modeling helps to:

- Identify relevant threats to a particular application scenario
- Identify key vulnerabilities in an application's design
- Improve security design

When using this approach, an administrator should keep the following in mind:

- Try not to be rigid about specific steps or implementations; instead, focus on the approach. If any step becomes impassable, go right to step 4 of the threat modeling process and identify the problem.
- Use scenarios to scope the modeling activity.
- Use existing design documents. Use items like documented use cases or use stories, architectural diagrams, data flow diagrams, or other design documentation.
- Start with a whiteboard before capturing information in documents or getting lost in details. It may be helpful to use a digital camera with printing capabilities to document and distribute the information from the whiteboard.

- Use an iterative approach. Add more details and improve the threat model as design and development continue. This will help with becoming familiar with the modeling process and developing the threat model to better examine more possible scenarios.
- Obtain input about the host and network constraints from the system and network administrators. To better understand the end-to-end deployment diagram, obtain as much information as possible about host configurations, firewall policies, allowed protocols and ports, and other relevant details.

The threat modeling process involves five steps:

1. **Identify Security Objectives**

   Security objectives are the goals and constraints related to the application's confidentiality, integrity, and availability. Security-specific objectives guide the threat modeling efforts and help to determine how much effort needs to be put toward subsequent steps. To identify security objectives, administrators should ask the following questions:

   - What data should be protected?
   - Are there any compliance requirements?
   - Are there specific quality-of-service requirements?
   - Are there intangible assets to protect?

2. **Application Overview**

   Identify the components, data flows, and trust boundaries. To draw the end-to-end deployment scenario, the administrator should use a whiteboard. First, they should draw a rough diagram that explains the workings and structure of the application, its subsystems, and its deployment characteristics. The deployment diagram should contain the following:

   - End-to-end deployment topology
   - Logical layers
   - Key components
   - Key services
   - Communication ports and protocols
   - Identities
   - External dependencies

   Identify Roles

   The administrator should identify people and the roles and actions they can perform within the application. For example, are there higher-privileged groups of users? Who can read data? Who can update data? Who can delete data?

Identify Key Usage Scenarios

The administrator should use the application's use cases to determine its objective. Use cases explain how the application is used and misused.

Identify Technologies

The administrator should list the technologies and key features of the software, as well as the following technologies in use:

- Operating systems
- Web server software
- Database server software
- Technologies for presentation, business, and data access layers
- Development languages

Identifying these technologies helps to focus on technology-specific threats.

Identify Application Security Mechanisms

The administrator should identify some key points regarding the following:

- Input and data validation
- Authorization and authentication
- Sensitive data
- Configuration management
- Session management
- Parameter manipulation
- Cryptography
- Exception management
- Auditing and logging

These efforts aim to identify relevant details and to add details where required, or to identify areas that require more.

3. Decompose the Application

In this step, the administrator breaks down the application to identify the trust boundaries, data flows, entry points, and exit points. Doing so makes it considerably easier to find more relevant and more detailed threats and vulnerabilities.

Identify Trust Boundaries

Identifying the application's trust boundaries helps the administrator to focus on the relevant areas of the application. It indicates where trust levels change.

- Identify outer system boundaries

- Identify access control points or key places where access requires extra privileges or role membership
- Identify trust boundaries from a data flow perspective

Identify Data Flows

The administrator should list the application's data input from entry to exit. This helps to understand how the application communicates with outside systems and clients and how the internal components interact. They should pay particular attention to the data flow across trust boundaries and the data validation at the trust boundary entry point. A good approach is to start at the highest level and then deconstruct the application by testing the data flow between different subsystems.

Identify Entry Points

The application's entry point can also serve as an entry point for attacks. All users interact with the application at these entry points. Other internal entry points uncovered by subcomponents over the layers of the application may be present only to support internal communication with other components. The administrator should identify these entry points to determine the methods used by an intruder to get in through them. They should focus on the entry points that allow access to critical functionalities and provide adequate defense for them.

Identify Exit Points

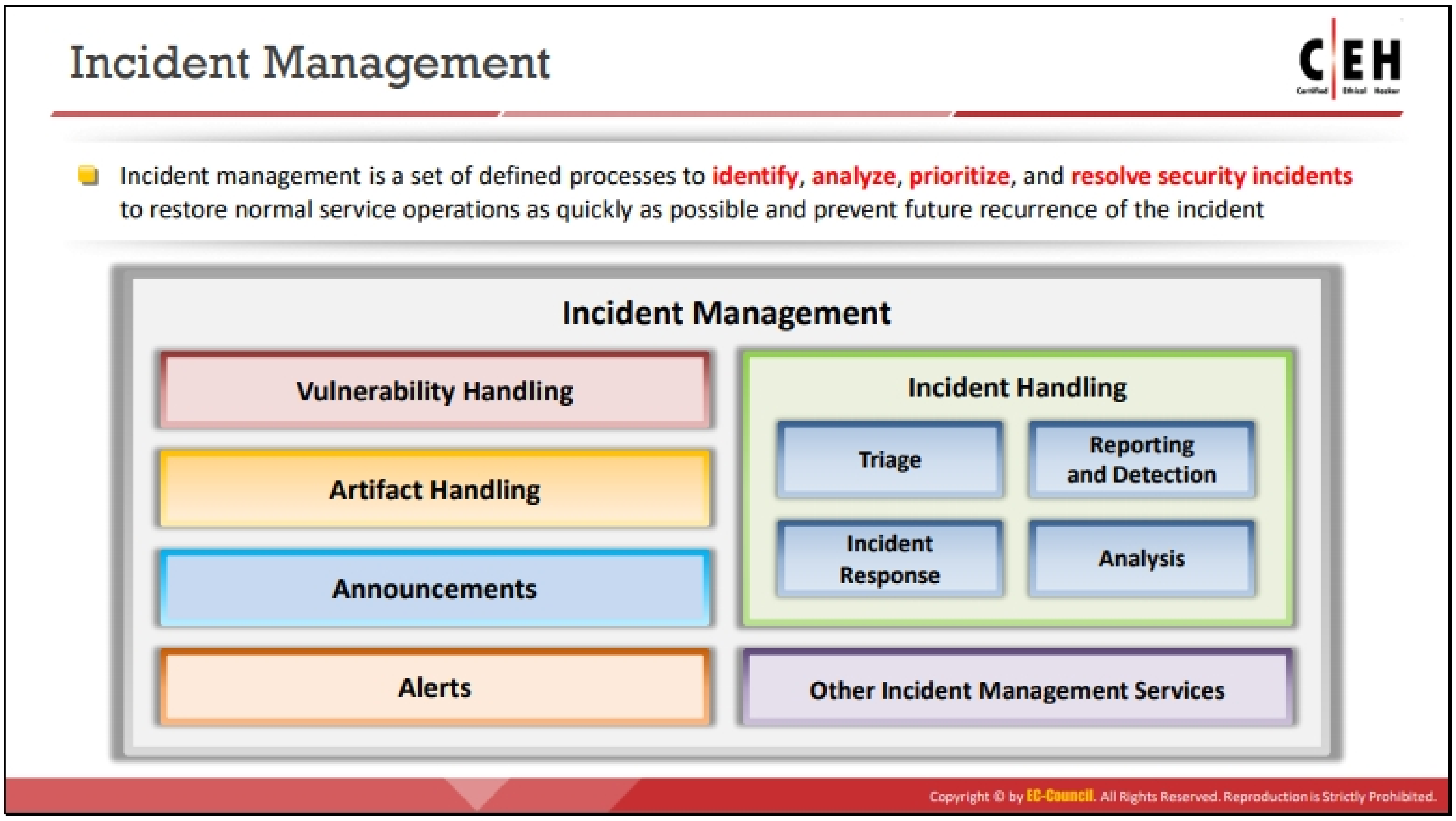
The administrator should also identify the points where the application transfers data to the client or external systems. They should prioritize the exit points at which the application writes data containing client input or data from untrusted sources, such as a shared database.

4. **Identify Threats**

The administrator should identify threats relevant to the control scenario and context using the information obtained in the application overview and decompose application steps. They should bring members of the development and test teams together to identify potential threats. The team should start with a list of common threats grouped by their application vulnerability category. This step uses a question-driven approach to help identify threats.

5. **Identify Vulnerabilities**

A vulnerability is a weakness in an application (deployed in an information system) that allows attacker exploitation, thereby leading to security breaches. Security administrators should identify any weaknesses related to the threats found using the vulnerability categories to identifying vulnerabilities and fix them beforehand to keep intruders away.



Incident Management

- Incident management is a set of defined processes to **identify**, **analyze**, **prioritize**, and **resolve security incidents** to restore normal service operations as quickly as possible and prevent future recurrence of the incident

Incident Management

Vulnerability Handling

Artifact Handling

Announcements

Alerts

Incident Handling

Triage

Reporting and Detection

Incident Response

Analysis

Other Incident Management Services

Incident Management

Incident management is a set of defined processes to identify, analyze, prioritize, and resolve security incidents to restore the system to normal service operations as soon as possible, and prevent recurrence of the incident. It involves not only responding to incidents but also triggering alerts to prevent potential risks and threats. A security administrator must identify software that is open to attacks before someone takes advantage of the vulnerabilities.

Incident management includes the following:

- Vulnerability analysis
- Artifact analysis
- Security awareness training
- Intrusion detection
- Public or technology monitoring

The incident management process is designed to:

- Improve service quality
- Resolve problems proactively
- Reduce the impact of incidents on an organization or its business
- Meet service availability requirements
- Increase staff efficiency and productivity
- Improve user and customer satisfaction
- Assist in handling future incidents

Conducting training sessions to spread awareness among users is an important part of incident management. Such sessions help end-users to recognize suspicious events or incidents easily and report an attacker's behavior to the appropriate authority.

The following people perform incident management activities:

- Human resources personnel take steps to fire employees suspected of harmful computer activities.
- The legal counsel sets the rules and regulations in an organization. These rules can influence the internal security policies and practices of the organization in case an insider or an attacker uses the organization's system for harmful or malicious activities.
- The firewall manager keeps filters in place. These filters are frequently where denial-of-service attacks are made.
- An outsourced service provider repairs systems infected by viruses and malware.

Incident response is one of the functions performed in incident handling. In turn, incident handling is one of the services provided as part of incident management. The following diagram illustrates the relationship between incident response, incident handling, and incident management.

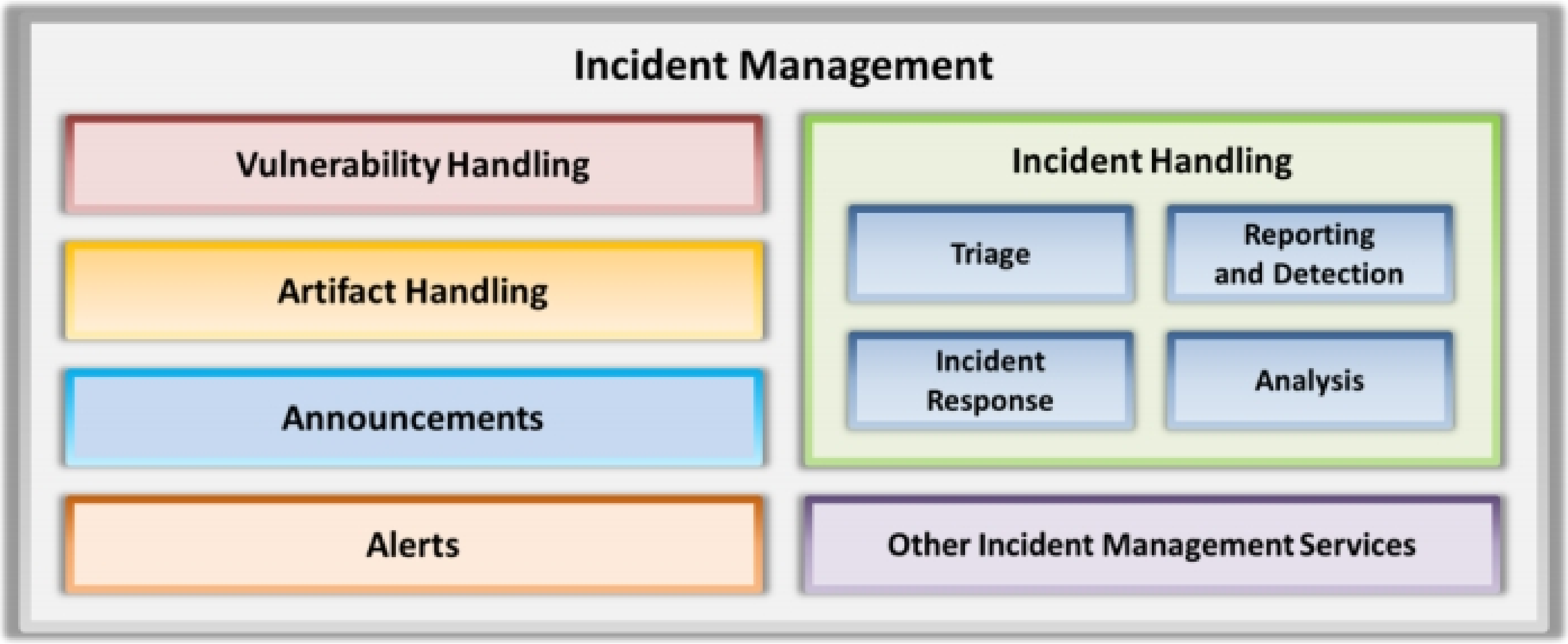
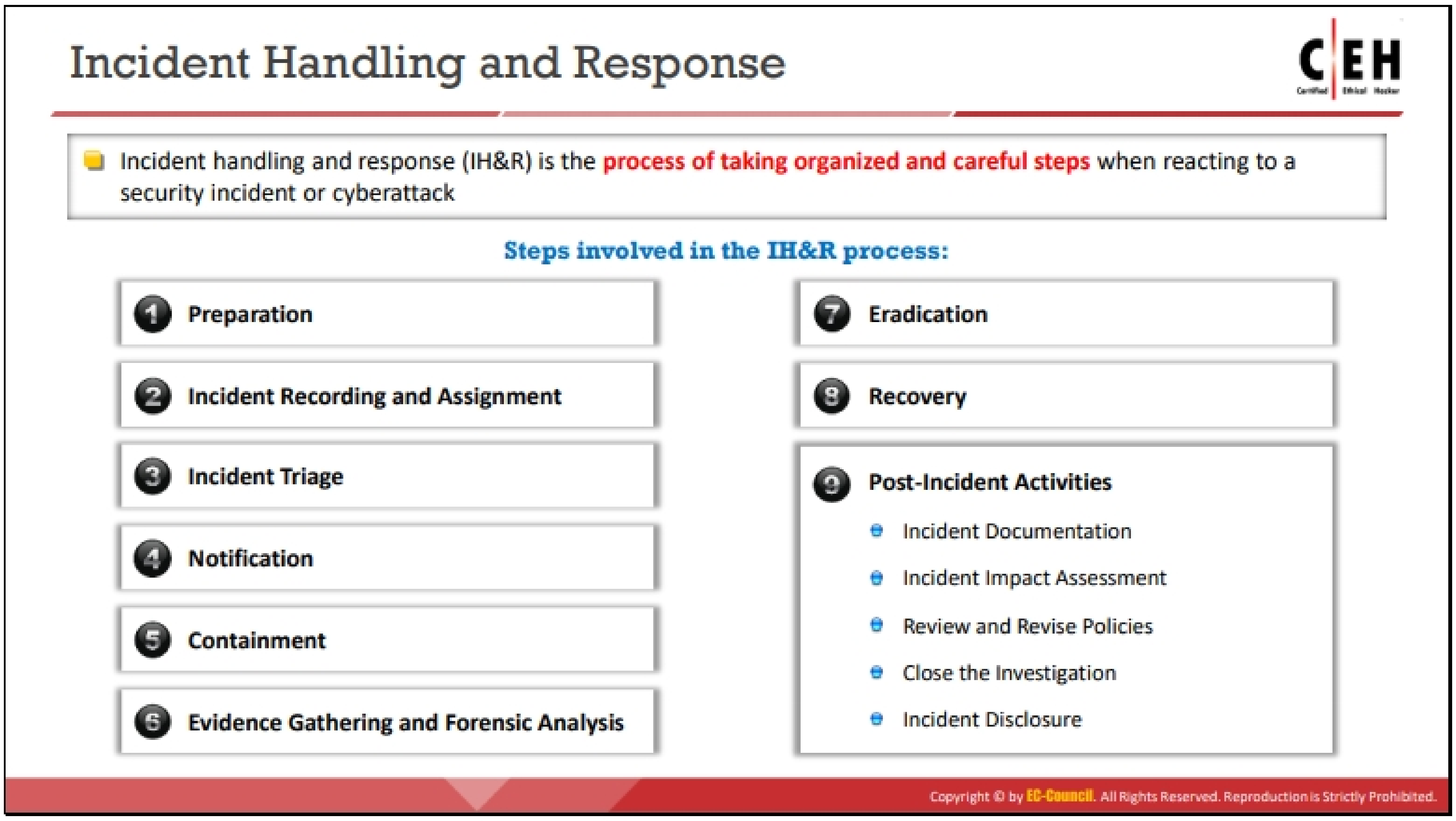

Incident Management
Vulnerability Handling
Artifact Handling
Announcements
Alerts
Incident Handling
Triage
Reporting and Detection
Incident Response
Analysis
Other Incident Management Services

Figure 1.4: Block Diagram of Incident Management



Incident Handling and Response

- Incident handling and response (IH&R) is the **process of taking organized and careful steps** when reacting to a security incident or cyberattack

Steps involved in the IH&R process:

1. **Preparation**
2. **Incident Recording and Assignment**
3. **Incident Triage**
4. **Notification**
5. **Containment**
6. **Evidence Gathering and Forensic Analysis**
7. **Eradication**
8. **Recovery**
9. **Post-Incident Activities**
   - Incident Documentation
   - Incident Impact Assessment
   - Review and Revise Policies
   - Close the Investigation
   - Incident Disclosure

Incident Handling and Response

Incident handling and response (IH&R) is the process of taking organized and careful steps when reacting to a security incident or cyberattack. It is a set of procedures, actions, and measures taken against an unexpected event occurrence. It involves logging, recording, and resolving incidents that take place in the organization. It notes the incident, when it occurred, its impact, and its cause. It is the practice of managing the incident response processes, such as preparation, detection, containment, eradication, and recovery, to overcome the impact of an incident quickly and efficiently. IH&R processes are important to provide a focused approach for restoring normal business operations as quickly as possible after an incident and with a minimal impact on the business.

The IH&R process involves defining user policies, developing protocols, building incident response teams, auditing organizational assets, planning incident response procedures, obtaining management approval, incident reporting, prioritization, and managing response. It also includes establishing proper communication between the individuals responding to an incident and guiding them to detect, analyze, contain, recover, and prevent incidents.

Discussed below are the steps involved in the IH&R process:

- **Step 1: Preparation**

  The preparation phase includes performing an audit of resources and assets to determine the purpose of security and define the rules, policies, and procedures that drive the IH&R process. It also includes building and training an incident response team, defining incident readiness procedures, and gathering required tools as well as training the employees to secure their systems and accounts.

- **Step 2: Incident Recording and Assignment**

  In this phase, the initial reporting and recording of the incident take place. This phase handles identifying an incident and defining proper incident communication plans for the employees and also includes communication methods that involve informing IT support personnel or submitting an appropriate ticket.

- **Step 3: Incident Triage**

  In this phase, the identified security incidents are analyzed, validated, categorized, and prioritized. The IH&R team further analyzes the compromised device to find incident details such as the type of attack, its severity, target, impact, and method of propagation, and any vulnerabilities it exploited.

- **Step 4: Notification**

  In the notification phase, the IH&R team informs various stakeholders, including management, third-party vendors, and clients, about the identified incident.

- **Step 5: Containment**

  This phase helps to prevent the spread of infection to other organizational assets, preventing additional damage.

- **Step 6: Evidence Gathering and Forensic Analysis**

  In this phase, the IH&R team accumulates all possible evidence related to the incident and submits it to the forensic department for investigation. Forensic analysis of an incident reveals details such as the method of attack, vulnerabilities exploited, security mechanisms averted, network devices infected, and applications compromised.

- **Step 7: Eradication**

  In the eradication phase, the IH&R team removes or eliminates the root cause of the incident and closes all the attack vectors to prevent similar incidents in the future.

- **Step 8: Recovery**

  After eliminating the causes for the incidents, the IH&R team restores the affected systems, services, resources, and data through recovery. It is the responsibility of the incident response team to ensure that that the incident causes no disruption to the services or business of the organization.

- **Step 9: Post-Incident Activities**

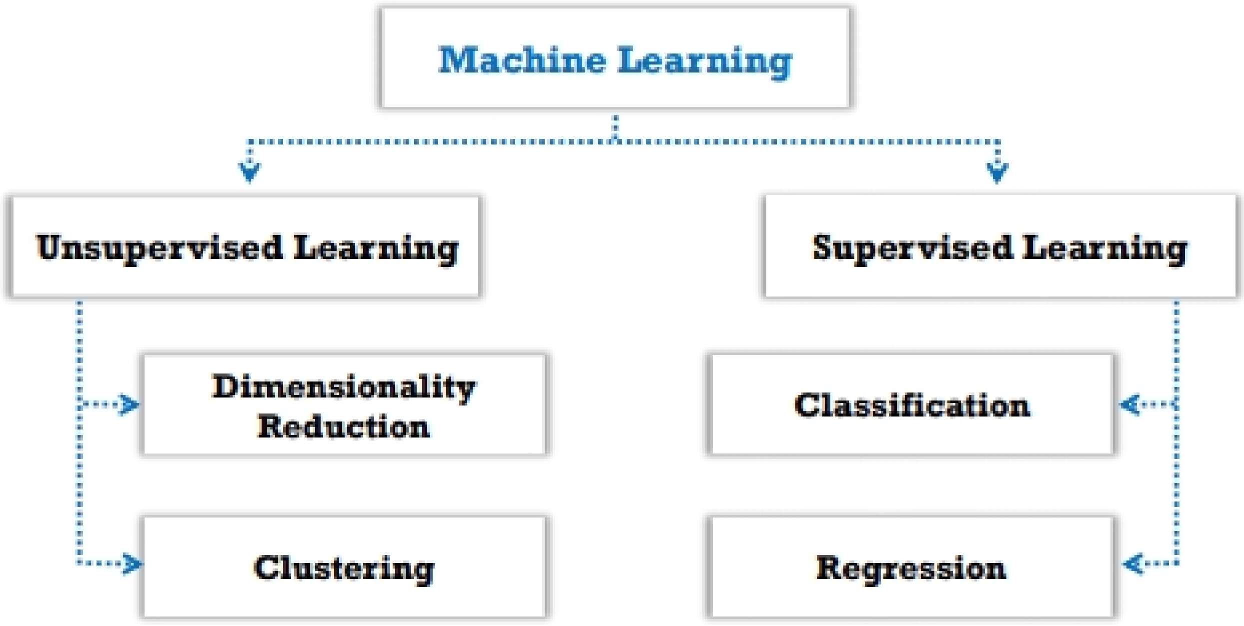
  Once the process is complete, the security incident requires additional review and analysis before closing the matter. Conducting a final review is an important step in the IH&R process that includes:

  - Incident documentation
  - Incident impact assessment
  - Reviewing and revising policies
  - Closing the investigation
  - Incident disclosure

Role of AI and ML in Cyber Security

- Machine learning (ML) and artificial intelligence (AI) are now vastly used across various industries and applications due to the **increase in computing power**, **data collection**, and **storage capabilities**
- ML is an **unsupervised self-learning system** that is used to define what the normal network looks like, along with its devices, and then to backtrack and **report any deviations or anomalies** in real-time
- AI and ML in cyber security helps in **identifying new exploits and weaknesses**, which can then be easily analyzed to mitigate further attacks

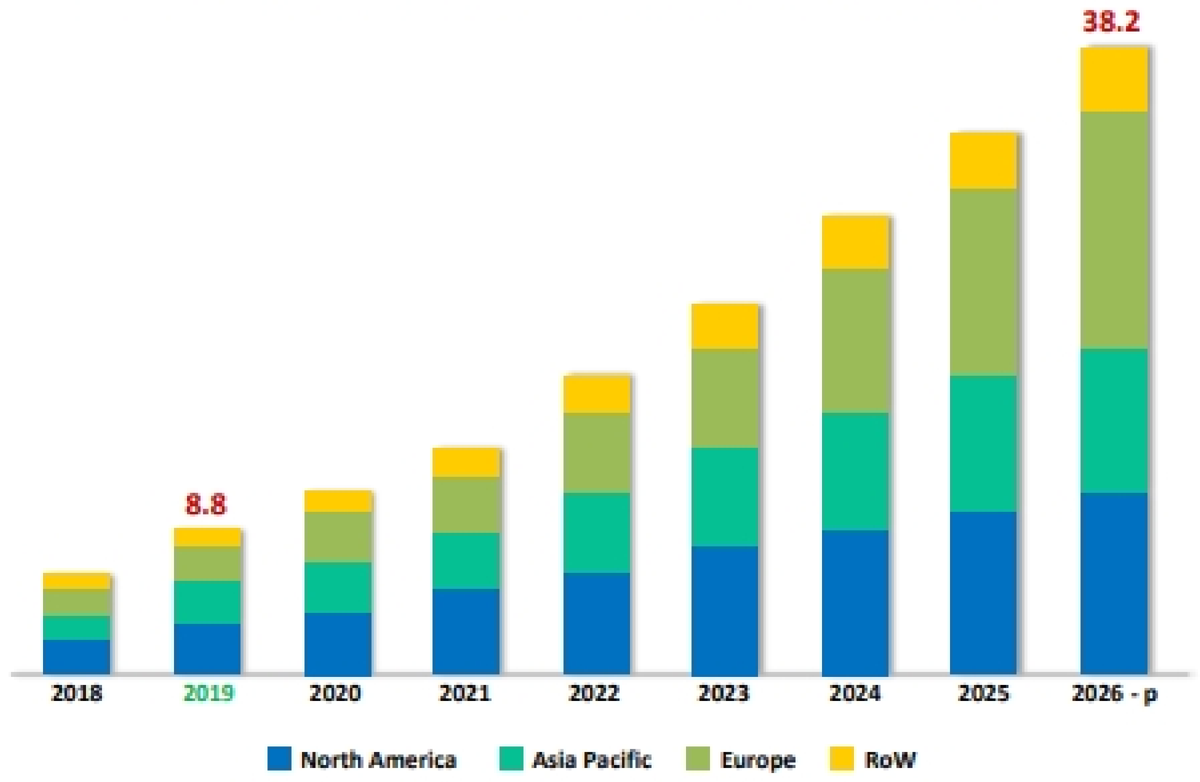
- ML classification techniques:
  - Supervised learning makes use of algorithms that input a **set of labeled training data**, with the aim of learning the differences between the labels
  - Unsupervised learning makes use of algorithms that input **unlabeled training data**, with the aim of deducing all categories by itself


Machine Learning
Unsupervised Learning
Supervised Learning
Dimensionality Reduction
Clustering
Classification
Regression

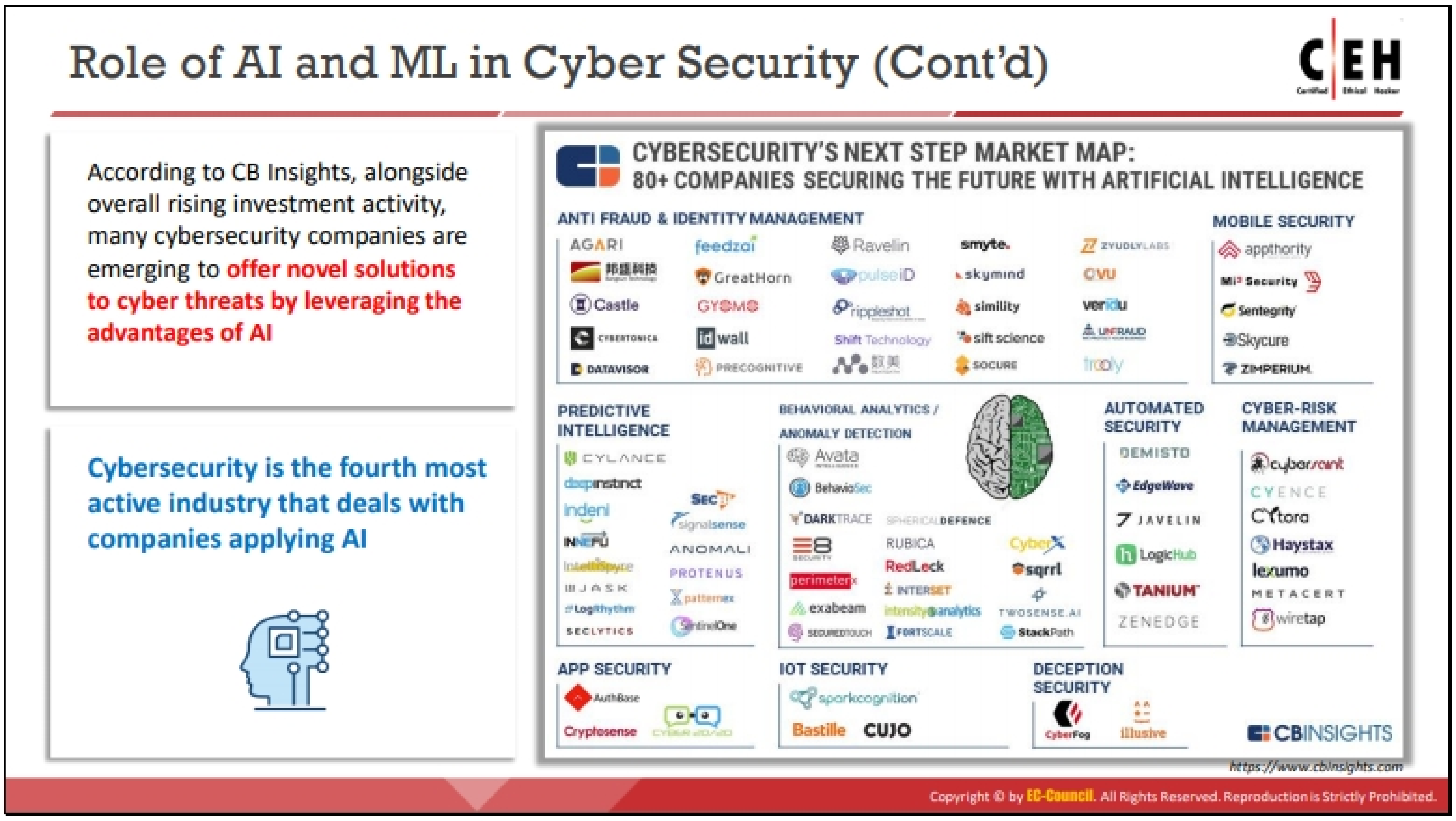
Role of AI and ML in Cyber Security (Cont'd)

- **The cyber security market is set to exceed $300 billion by 2024, and the AI-related cyber security market is predicted to reach a value of $38.2 billion by 2026**

AI in Cyber Security Market, by Region (USD Billion)



https://www.marketsandmarkets.com



Role of AI and ML in Cyber Security (Cont'd)

According to CB Insights, alongside overall rising investment activity, many cybersecurity companies are emerging to **offer novel solutions to cyber threats by leveraging the advantages of AI**

Cybersecurity is the fourth most active industry that deals with companies applying AI

CYBERSECURITY'S NEXT STEP MARKET MAP:
80+ COMPANIES SECURING THE FUTURE WITH ARTIFICIAL INTELLIGENCE
ANTI FRAUD & IDENTITY MANAGEMENT
AGARI
feedzai
Ravelin
smyte.
ZYUDLYLABS
GreatHorn
pulseID
skymind
CVU
Castle
GYOMO
rippleshot
simility
veridu
CYBERTONICA
idwall
Shift Technology
sift science
UNFRAUD
DATAVISOR
PRECOGNITIVE
SOCURE
trooly
MOBILE SECURITY
appthority
Mi3 Security
Sentegrity
Skycure
ZIMPERIUM
PREDICTIVE INTELLIGENCE
CYLANCE
deepinstinct
SECDO
indeni
signalsense
INNEFU
ANOMALI
Intellispyce
PROTENUS
JASK
patternex
LogRhythm
SentinelOne
SECLYTICS
BEHAVIORAL ANALYTICS / ANOMALY DETECTION
Avata
BehavioSec
DARKTRACE
SPHERICALDEFENCE
E8 SECURITY
RUBICA
CyberX
perimeterx
RedLock
sqrrl
INTERSET
exabeam
intensityanalytics
TWOSENSE.AI
SECUREDTOUCH
FORTSCALE
StackPath
AUTOMATED SECURITY
DEMISTO
EdgeWave
JAVELIN
LogicHub
TANIUM
ZENEDGE
CYBER-RISK MANAGEMENT
cybersponse
CYENCE
Cytora
Haystax
lexumo
METACERT
wiretap
APP SECURITY
AuthBase
Cryptosense
CYBER ADAPT
IOT SECURITY
sparkcognition
Bastille
CUJO
DECEPTION SECURITY
CyberFog
illusive
CBINSIGHTS

https://www.cbinsights.com

Role of AI and ML in Cyber Security

Machine learning (ML) and Artificial Intelligence (AI) are now popularly used across various industries and applications due to the increase in computing power, data collection, and storage capabilities.

Along with technological advancements in AI, such as self-driving cars, language translators, and big data, there is also a rise in threats such as ransomware, botnets, malware, and phishing. Using AI and ML in cybersecurity helps to identify new exploits and weaknesses, which can be easily analyzed to mitigate further attacks. It reduces the pressure on security professionals and alerts them whenever an action is needed.

What are AI and ML?

Artificial Intelligence is the only solution to defend networks against the various attacks that an antivirus scan cannot detect. A huge amount of collected data is fed into the AI, which processes and analyzes it to understand its details and trends.

ML is a branch of artificial intelligence (AI) that gives the systems the ability to self-learn without any explicit programs. This self-learning system is used to define what the normal network, along with its devices, looks like, and then uses this to backtrack and report any deviations or anomalies in real-time.

There are two types of ML classification techniques:

- **Supervised Learning**

  Supervised learning uses algorithms that input a set of labeled training data to attempt to learn the differences between the given labels. Supervised learning is further divided into two subcategories, namely, classification and regression. Classification includes completely divided classes. Its main task is to define the test sample to identify its class. Regression is used when data classes are not separated, such as when the data is continuous.

- **Unsupervised Learning**

  Unsupervised learning makes use of algorithms that input unlabeled training data to attempt to deduce all the categories without guidance. Unsupervised learning is further divided into two subcategories, namely, clustering and dimensionality reduction. Clustering divides the data into clusters based on their similarities, regardless of class information. Dimensionality reduction is the process of reducing the dimensions (attributes) of data.

Why AI and ML?

Source: *https://www.gartner.com*, *https://www.marketsandmarkets.com*

The security threat landscape continues to evolve not just in scale, but, more importantly, in sophistication. Despite a range of advancements in the industry to safeguard against increasingly bold and intricate threats, organizations have struggled to keep pace with the technologies and techniques employed by attackers.

As companies continue to increase their digital footprints, “identify and diagnose” capabilities are not enough to remediate against this growing fundamental business challenge for organizations of all shapes and sizes. The development of advanced security analytics is an important consideration for organizations looking to implement machine learning to defend against an array of internal and external security threats.

The cyber security market is set to exceed $300 billion by 2024, and the AI-related cyber security market is predicted to reach a value of $38.2 billion by 2026.

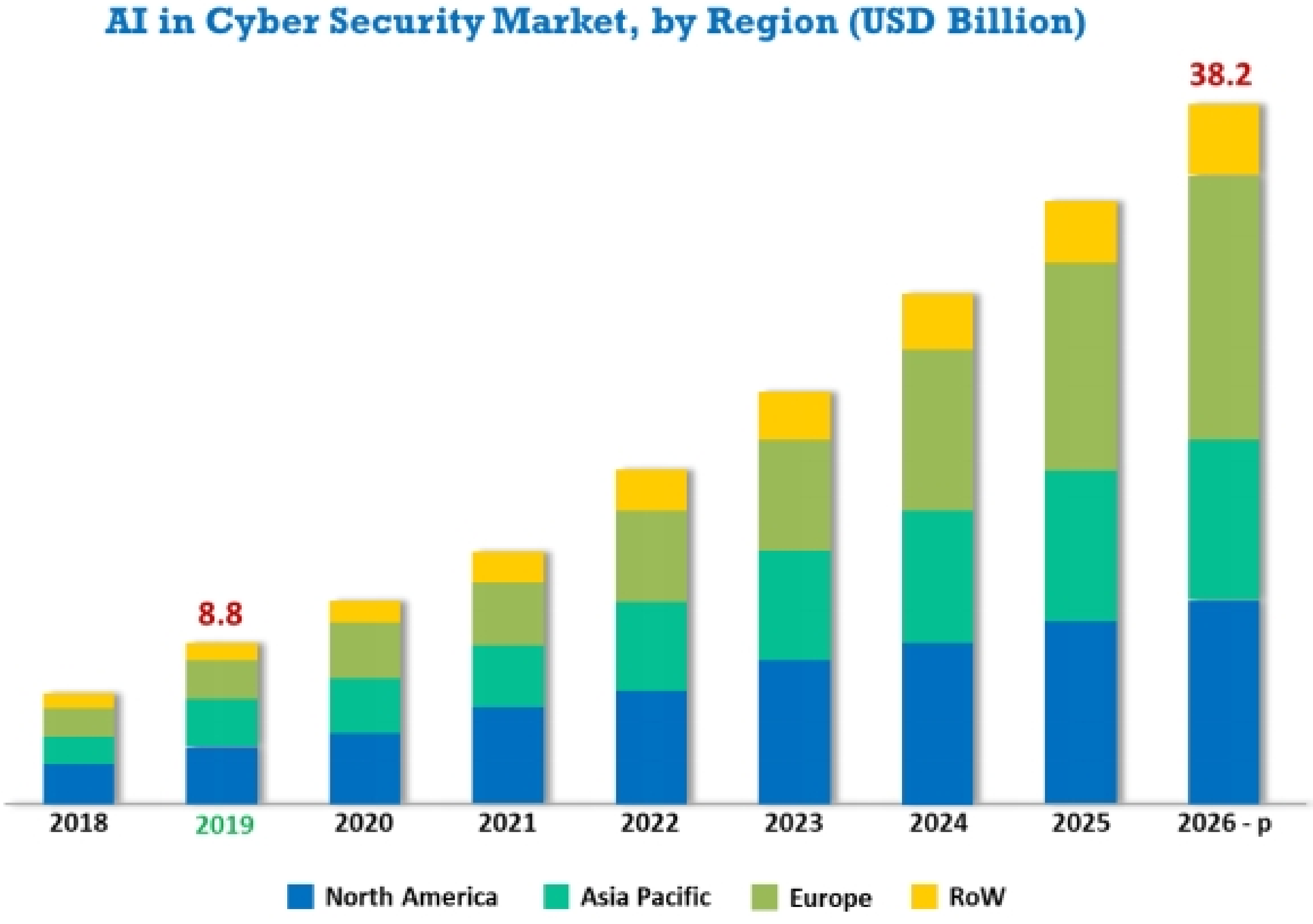


Figure 1.5: AI in Cyber Security Market

AI and ML Application Areas

Source: *https://www.cbinsights.com*

According to CB Insights, alongside overall rising investment activity, many cybersecurity companies are emerging to offer novel solutions to cyber threats by leveraging the advantages of artificial intelligence (AI).

According to CB Insights' AI Deals Tracker, cybersecurity is the fourth most active industry for deals to companies applying AI. As per CB Insights' data, there are over 80 private companies in cybersecurity that are using AI, categorized into the nine main areas in which they operate:

- Anti-fraud and identity management
- Mobile security
- Predictive intelligence
- Behavioral analytics and anomaly detection
- Automated security
- Cyber-risk management
- App security
- IoT security
- Deception security

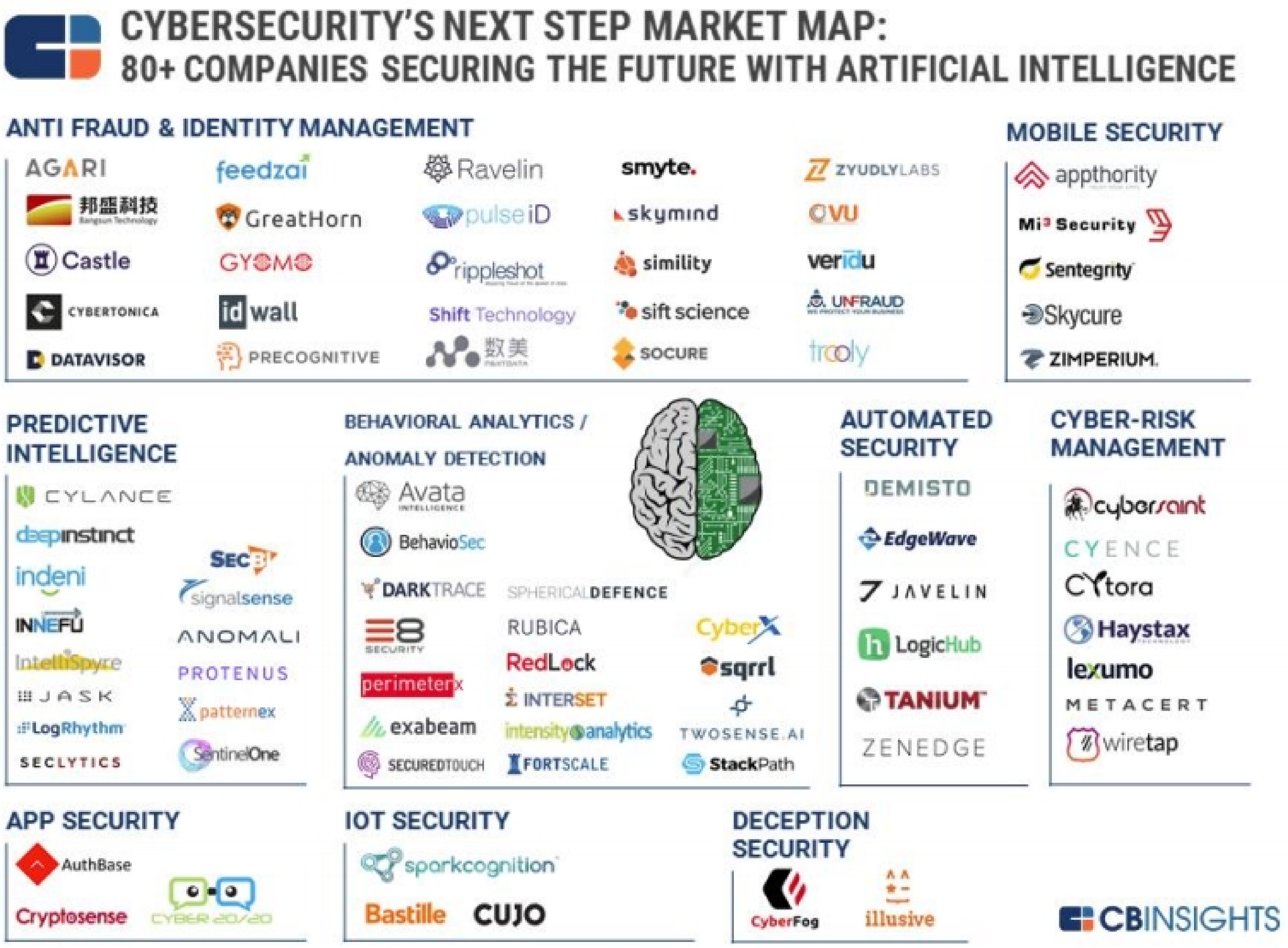
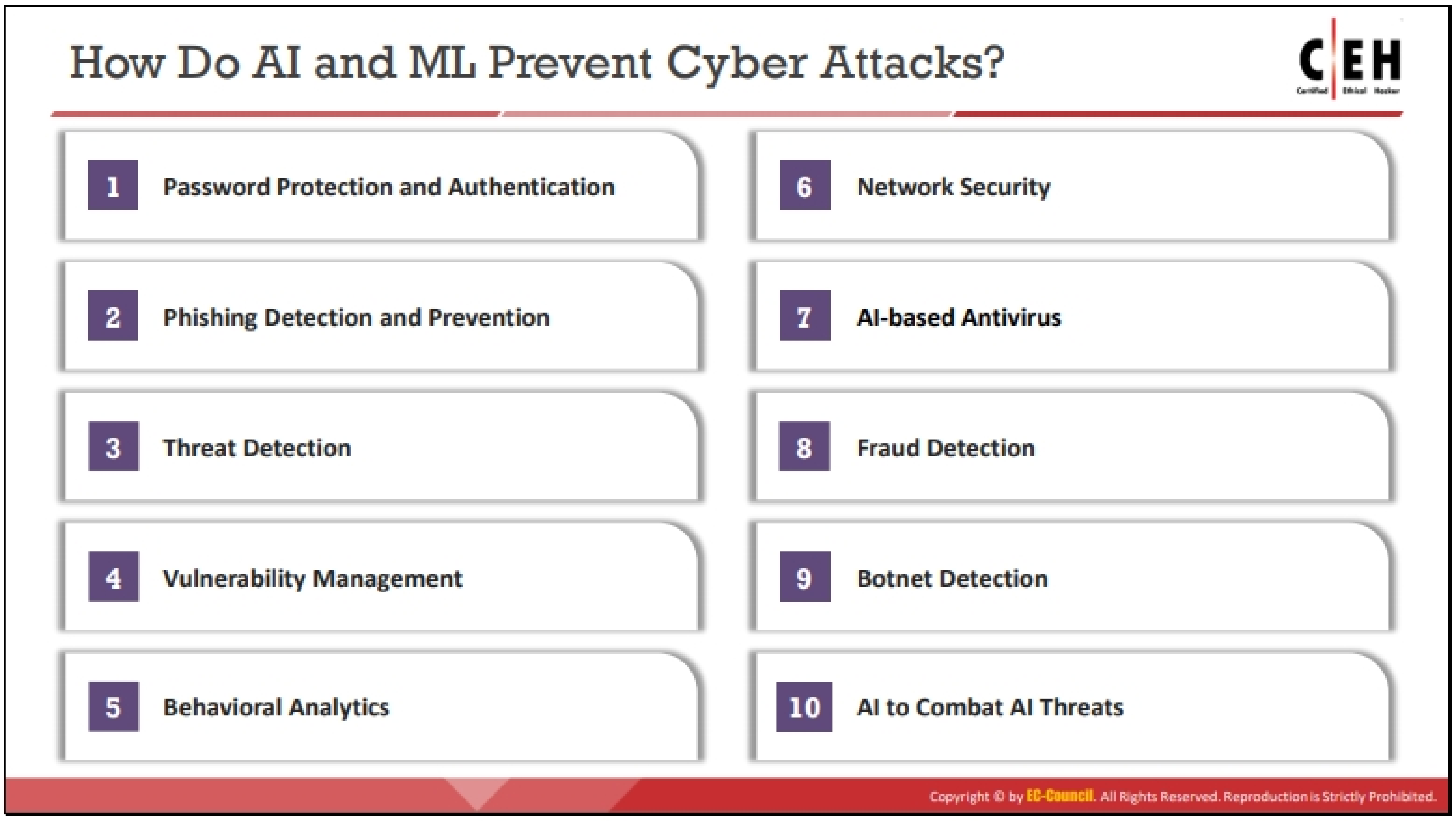

CYBERSECURITY'S NEXT STEP MARKET MAP:
80+ COMPANIES SECURING THE FUTURE WITH ARTIFICIAL INTELLIGENCE
ANTI FRAUD & IDENTITY MANAGEMENT
AGARI
邦盛科技
Castle
CYBERTONICA
DATAVISOR
feedzai
GreatHorn
GYOMO
idwall
PRECOGNITIVE
Ravelin
pulseiD
rippleshot
Shift Technology
数美
smyte.
skymind
simility
sift science
SOCURE
ZYUDLYLABS
OVU
veridu
UNFRAUD
trooly
MOBILE SECURITY
appthority
Mi3 Security
Sentegrity
Skycure
ZIMPERIUM.
PREDICTIVE INTELLIGENCE
CYLANCE
deepinstinct
indeni
INNEFU
IntelliSpyre
JASK
LogRhythm
SECLYTICS
SECBI
signalsense
ANOMALI
PROTENUS
patternex
SentinelOne
BEHAVIORAL ANALYTICS / ANOMALY DETECTION
Avata
BehavioSec
DARKTRACE
E8 SECURITY
perimeterx
exabeam
SECUREDTOUCH
SPHERICALDEFENCE
RUBICA
RedLock
INTERSET
intensityanalytics
FORTSCALE
CyberX
sqrrl
TWOSENSE.AI
StackPath
AUTOMATED SECURITY
DEMISTO
EdgeWave
JAVELIN
LogicHub
TANIUM
ZENEDGE
CYBER-RISK MANAGEMENT
cybersaint
CYENCE
CYtora
Haystax
lexumo
METACERT
wiretap
APP SECURITY
AuthBase
Cryptosense
CYBER 20/20
IOT SECURITY
sparkcognition
Bastille
CUJO
DECEPTION SECURITY
CyberFog
illusive
CBINSIGHTS

Figure 1.6: Companies using Artificial Intelligence



How Do AI and ML Prevent Cyber Attacks?

1. Password Protection and Authentication
2. Phishing Detection and Prevention
3. Threat Detection
4. Vulnerability Management
5. Behavioral Analytics
6. Network Security
7. AI-based Antivirus
8. Fraud Detection
9. Botnet Detection
10. AI to Combat AI Threats

How Do AI and ML Prevent Cyber Attacks?

Artificial Intelligence (AI), and with it, Machine Learning (ML), is an emerging technology in the field of cybersecurity. It is widely adopted by largescale industries such as automation, IT services, manufacturing, production, and finance. AI plays a crucial role in detecting imminent cyber threats by incorporating machine learning as a subset.

Following are different ways that AI and ML safeguard industries from cybersecurity attacks:

- **Password Protection and Authentication**

  Password credentials play a critical role in preventing illegitimate access to the organization's or user's data. If credentials are compromised, the reputation of the organization or person could be damaged. Sometimes, traditional face detection and other biometric security measures can also be vulnerable to these credential breaches. Programmers use AI to improve biometric validations and face recognition to thwart such attacks. AI provides the latest models for recognizing an individual's face by tracking key correlations and patterns.

- **Phishing Detection and Prevention**

  Phishing is a common method attackers employ to send their payloads via emails. The majority of users cannot figure out which received emails have a malicious attachment or payload. In this case, AI and ML could play a pivotal role in identifying and preventing such phishing attacks. They can scan and identify phishing emails much faster than a human being can. They can also quickly differentiate malicious websites from legitimate websites.

- **Threat Detection**

  Machine learning assists companies in detecting cyber-attacks before systems are compromised. Being a part of AI, machine learning constantly keeps admins notified of imminent cyber threats by carrying out logical data analysis. ML allows systems to run its algorithms upon the data being received, then performs deep learning on the and comprehends the advancements required to ensure the safety of the information systems.

- **Vulnerability Management**

  AI and ML-based systems never allow vulnerability to exist for long; they dynamically scan for all types of vulnerabilities and alert the admins before the system is exploited. They can also provide the attacker's information and the patterns used to perform the attack. These AI- and ML-based systems can also forecast how and when a vulnerability exploitation might occur.

- **Behavioral Analytics**

  Another notable security improvement by artificial intelligence is "Behavioral Analytics." Attackers who have stolen the credentials of a legitimate user can perform malicious activities on the organization's network; such attempts are difficult to detect and thwart. Here, AI with ML generates specific user patterns based on their regular usage. AI software instantly alerts the admin if it detects any suspicious activity or deviation in regular usage.

- **Network Security**

  Two significant factors of network security are generating comprehensive security policies and mapping an enterprise's network topology. Unfortunately, both of these factors are time-consuming. Therefore, administrators are adopting AI to enhance this operation; it can carry out the network traffic analysis and propose efficient security policies by default.

- **AI-based Antivirus**

  Traditional antivirus tools perform file scanning on the organization's networks to check if any signatures match those of known viruses or malware. The issue with this is that antivirus tools must be updated when the user wants to scan for new malware or viruses. Updating is time-consuming, and new deployment often takes a certain amount of time. To overcome these issues, organizations employ AI-based antiviruses, which use anomaly detection to understand programs' behavior. AI-based antivirus detects suspicious program behavior instead of matching signatures for viruses.

- **Fraud Detection**

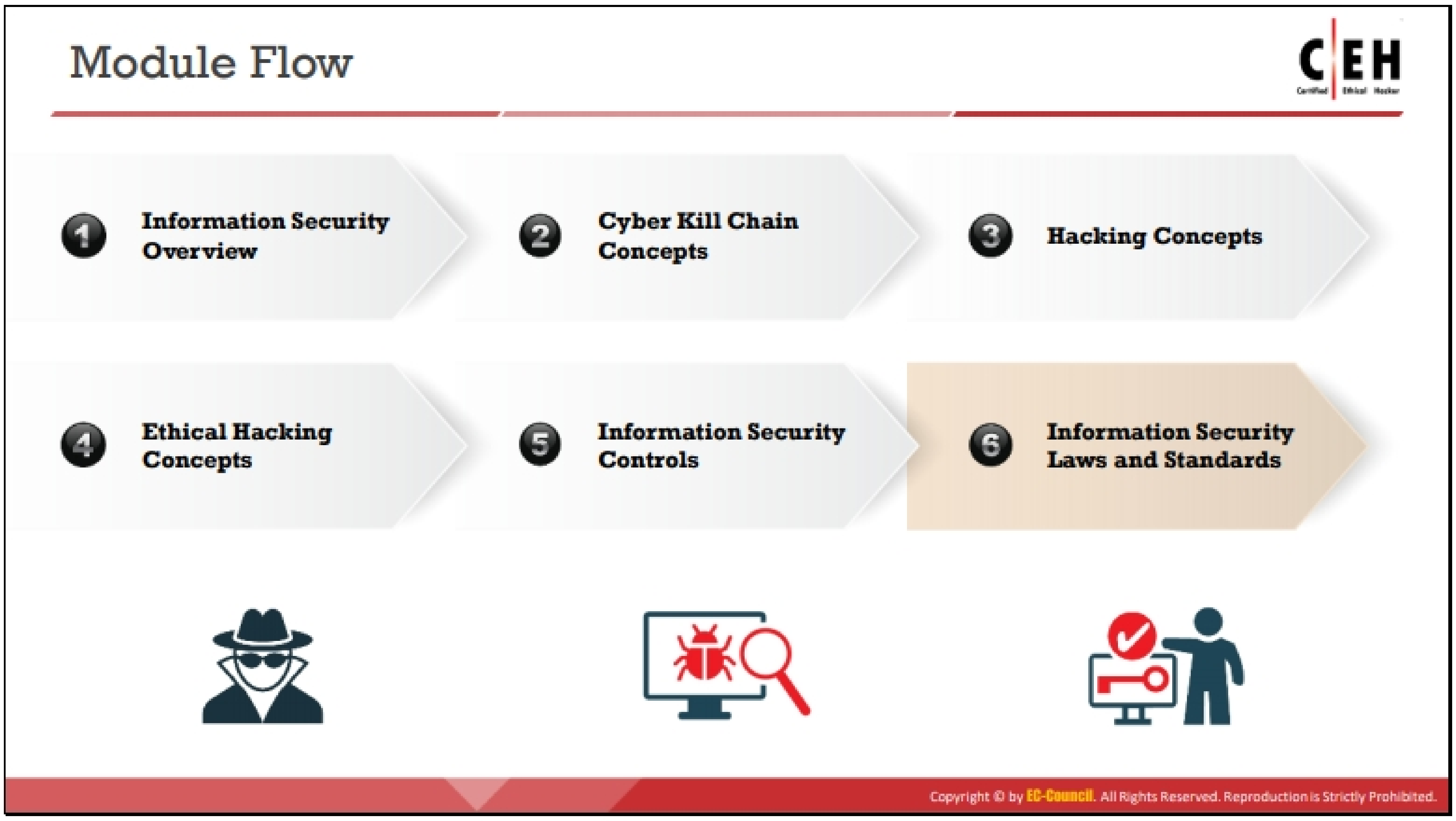
  AI and ML algorithms carry out anomaly detection to identify payment inconsistencies and fraudulent transactions. They also perform automated pattern discovery across different transactions. ML can easily differentiate between authentic and illegitimate transactions and blocks fraudulent transactions.

- **Botnet Detection**

  Botnets can bypass the Instruction Detection System (IDS) by leveraging its ineffectiveness in matching signatures. Botnets can be embedded using a highly sophisticated code that makes them untraceable by traditional IDS implementations. Hence, security professionals use AI and ML algorithms that alert about the suspicious behavior of a network and detect unauthorized intrusions.

- **AI to Combat AI Threats**

  Attackers can also leverage AI technology to make their way into an organization's network; such cyber threats must be detected immediately. AI software can detect such imminent AI-augmented attacks before the network is compromised.

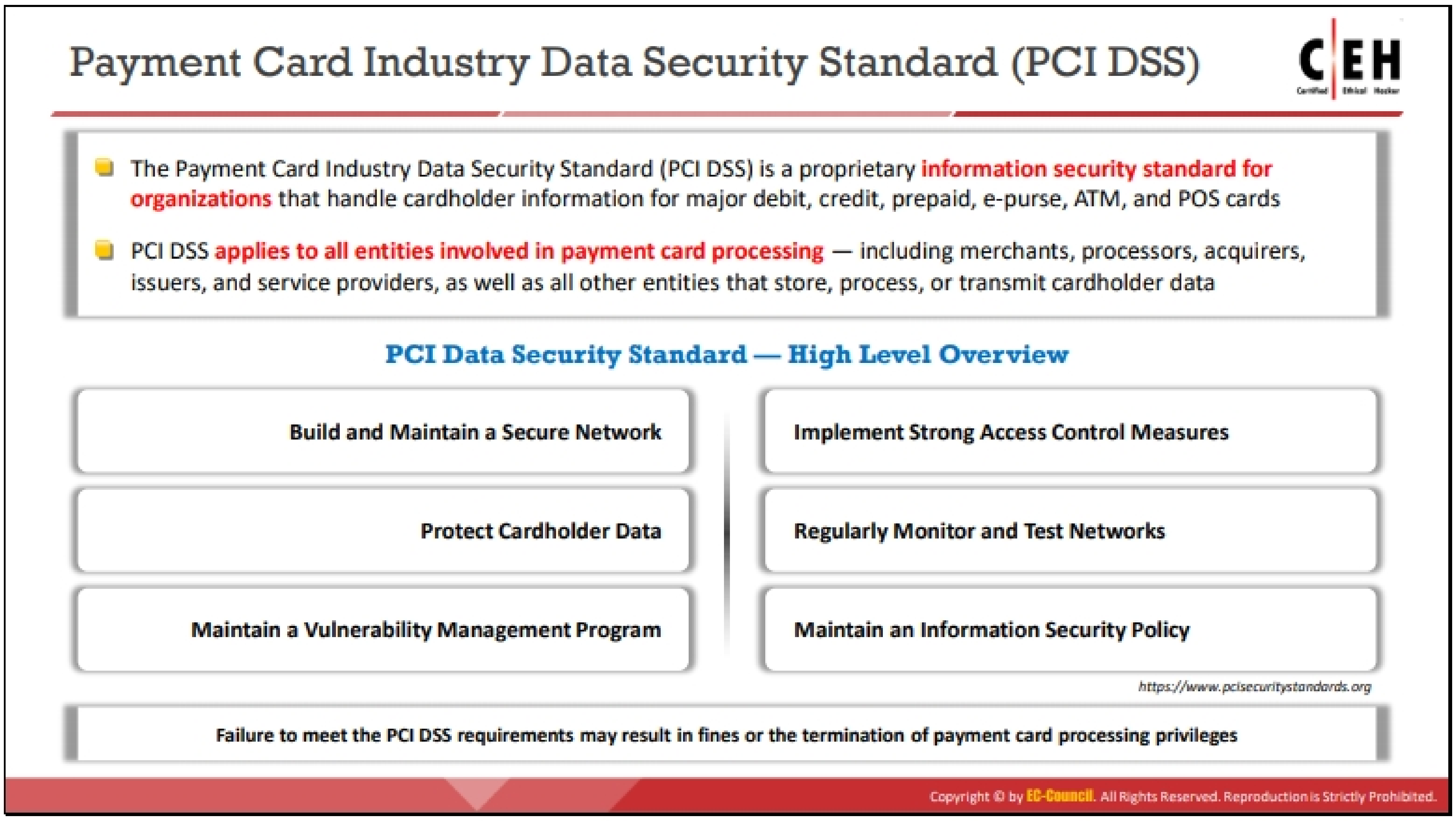


Module Flow

1. Information Security Overview
2. Cyber Kill Chain Concepts
3. Hacking Concepts
4. Ethical Hacking Concepts
5. Information Security Controls
6. Information Security Laws and Standards

Information Security Laws and Standards

Laws are a system of rules and guidelines that are enforced by a particular country or community to govern behavior. A Standard is a "document established by consensus and approved by a recognized body that provides, for common and repeated use, rules, guidelines, or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context." This section deals with the various laws and standards dealing with information security in different countries.



Payment Card Industry Data Security Standard (PCI DSS)

- The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary **information security standard for organizations** that handle cardholder information for major debit, credit, prepaid, e-purse, ATM, and POS cards
- PCI DSS **applies to all entities involved in payment card processing** — including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process, or transmit cardholder data

PCI Data Security Standard — High Level Overview

- **Build and Maintain a Secure Network**
- **Protect Cardholder Data**
- **Maintain a Vulnerability Management Program**
- **Implement Strong Access Control Measures**
- **Regularly Monitor and Test Networks**
- **Maintain an Information Security Policy**

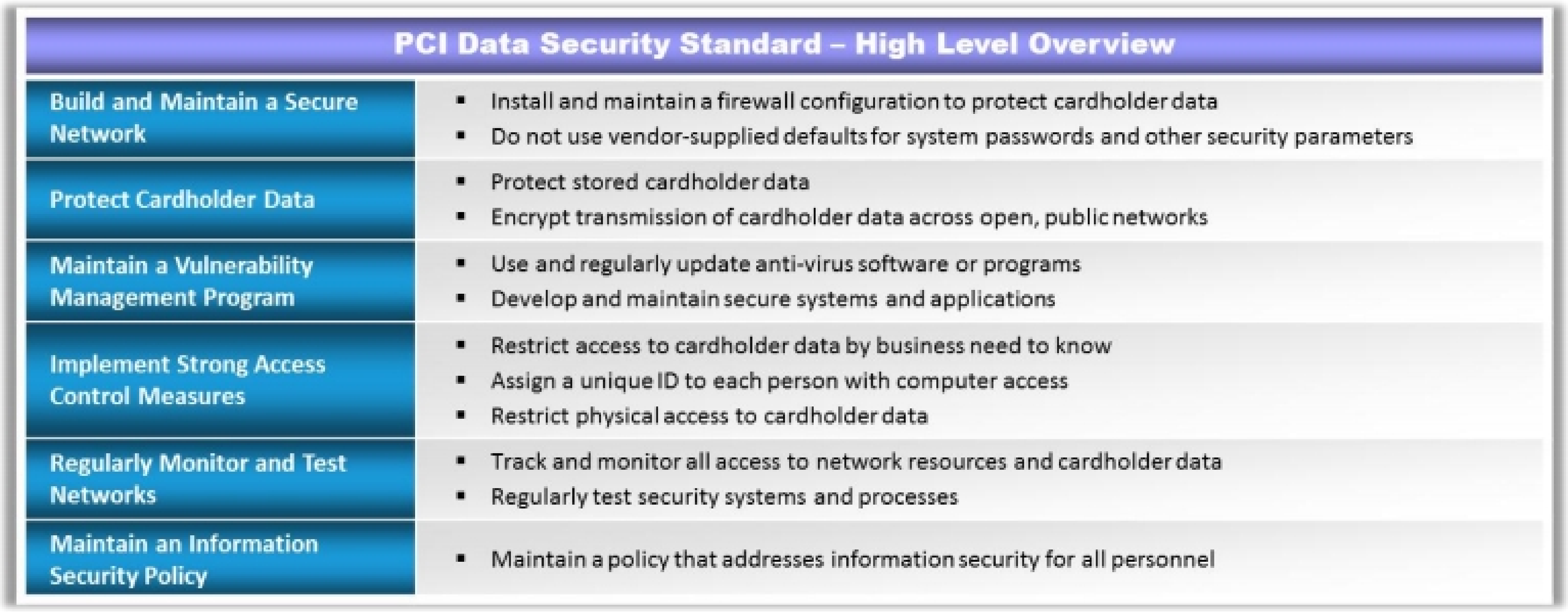
https://www.pcisecuritystandards.org

Failure to meet the PCI DSS requirements may result in fines or the termination of payment card processing privileges

Payment Card Industry Data Security Standard (PCI DSS)

Source: *https://www.pcisecuritystandards.org*

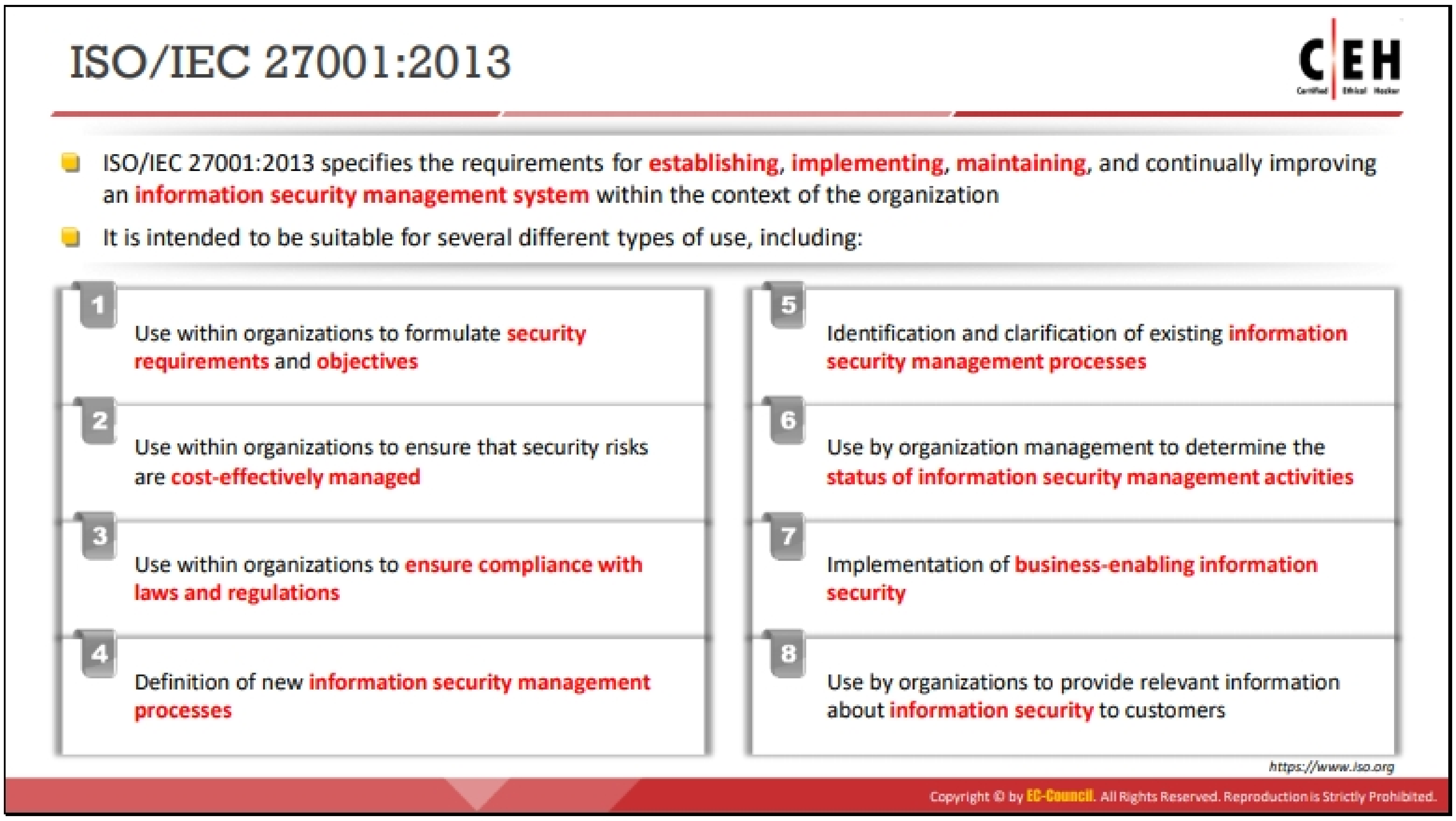
The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards. This standard offers robust and comprehensive standards and supporting materials to enhance payment card data security. These materials include a framework of specifications, tools, measurements, and support resources to help organizations ensure the safe handling of cardholder information. PCI DSS applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data. PCI DSS comprises a minimum set of requirements for protecting cardholder data. The Payment Card Industry (PCI) Security Standards Council has developed and maintains a high-level overview of PCI DSS requirements.



PCI Data Security Standard – High Level Overview	
Build and Maintain a Secure Network	▪ Install and maintain a firewall configuration to protect cardholder data ▪ Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	▪ Protect stored cardholder data ▪ Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	▪ Use and regularly update anti-virus software or programs ▪ Develop and maintain secure systems and applications
Implement Strong Access Control Measures	▪ Restrict access to cardholder data by business need to know ▪ Assign a unique ID to each person with computer access ▪ Restrict physical access to cardholder data
Regularly Monitor and Test Networks	▪ Track and monitor all access to network resources and cardholder data ▪ Regularly test security systems and processes
Maintain an Information Security Policy	▪ Maintain a policy that addresses information security for all personnel

Table 1.3: Table Showing the PCI Data Security Standard—High-Level Overview

Failure to meet PCI DSS requirements may result in fines or the termination of payment-card processing privileges.



ISO/IEC 27001:2013

- ISO/IEC 27001:2013 specifies the requirements for **establishing**, **implementing**, **maintaining**, and continually improving an **information security management system** within the context of the organization
- It is intended to be suitable for several different types of use, including:

1. Use within organizations to formulate **security requirements** and **objectives**
2. Use within organizations to ensure that security risks are **cost-effectively managed**
3. Use within organizations to **ensure compliance with laws and regulations**
4. Definition of new **information security management processes**
5. Identification and clarification of existing **information security management processes**
6. Use by organization management to determine the **status of information security management activities**
7. Implementation of **business-enabling information security**
8. Use by organizations to provide relevant information about **information security** to customers

https://www.iso.org

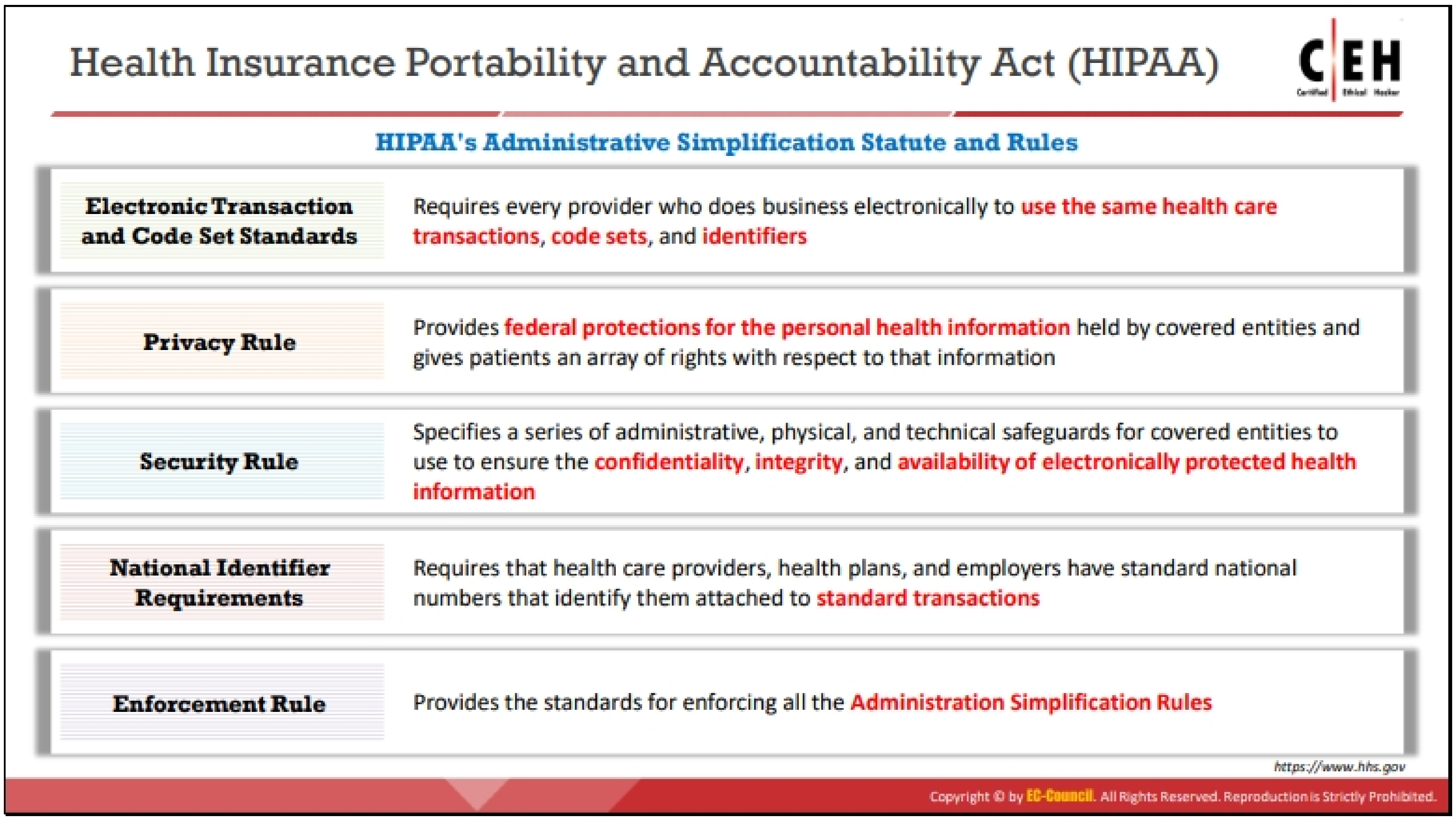
ISO/IEC 27001:2013

Source: *https://www.iso.org*

ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of an organization. It includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.

The regulation is intended to be suitable for several different uses, including:

- Use within organizations to formulate security requirements and objectives
- Use within organizations as a way to ensure that security risks are cost-effectively managed
- Use within organizations to ensure compliance with laws and regulations
- Defining new information security management processes
- Identifying and clarifying existing information security management processes
- Use by the management of organizations to determine the status of information security management activities
- Implementing business-enabling information security
- Use by organizations to provide relevant information about information security to customers



Health Insurance Portability and Accountability Act (HIPAA)

HIPAA's Administrative Simplification Statute and Rules

Electronic Transaction and Code Set Standards	Requires every provider who does business electronically to **use the same health care transactions**, **code sets**, and **identifiers**
Privacy Rule	Provides **federal protections for the personal health information** held by covered entities and gives patients an array of rights with respect to that information
Security Rule	Specifies a series of administrative, physical, and technical safeguards for covered entities to use to ensure the **confidentiality**, **integrity**, and **availability of electronically protected health information**
National Identifier Requirements	Requires that health care providers, health plans, and employers have standard national numbers that identify them attached to **standard transactions**
Enforcement Rule	Provides the standards for enforcing all the **Administration Simplification Rules**

https://www.hhs.gov

Health Insurance Portability and Accountability Act (HIPAA)

Source: *https://www.hhs.gov*

The HIPAA Privacy Rule provides federal protections for the individually identifiable health information held by covered entities and their business associates and gives patients an array of rights to that information. At the same time, the Privacy Rule permits the disclosure of health information needed for patient care and other necessary purposes.

The Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities and their business associates to use to ensure the confidentiality, integrity, and availability of electronically protected health information.

The office of civil rights implemented HIPAA's Administrative Simplification Statute and Rules, as discussed below:

- **Electronic Transactions and Code Set Standards**

  Transactions are electronic exchanges involving the transfer of information between two parties for specific purposes. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) designated certain types of organizations as covered entities, including health plans, health care clearinghouses, and certain health care providers. In the HIPAA regulations, the Secretary of Health and Human Services (HHS) adopted certain standard transactions for the Electronic Data Interchange (EDI) of health care data. These transactions are claims and encounter information, payment and remittance advice, claim status, eligibility, enrollment and disenrollment, referrals and authorizations, coordination of benefits, and premium payment. Under HIPAA, if a covered entity electronically conducts one of the adopted transactions, they must use the adopted standard—either from ASC, X12N, or NCPDP (for certain pharmacy transactions). Covered entities must adhere to the content and format requirements of each transaction. Every provider who does business electronically must use the same health care transactions, code sets, and identifiers.

- **Privacy Rule**

  The HIPAA Privacy Rule establishes national standards to protect people's medical records and other personal health information and applies to health plans, health care clearinghouses, and health care providers that conduct certain health care transactions electronically. The rule requires appropriate safeguards to protect the privacy of personal health information. It sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The rule also gives patients rights over their health information, including the right to examine and obtain a copy of their health records and to request corrections.

- **Security Rule**

  The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronically protected health information.

- **Employer Identifier Standard**

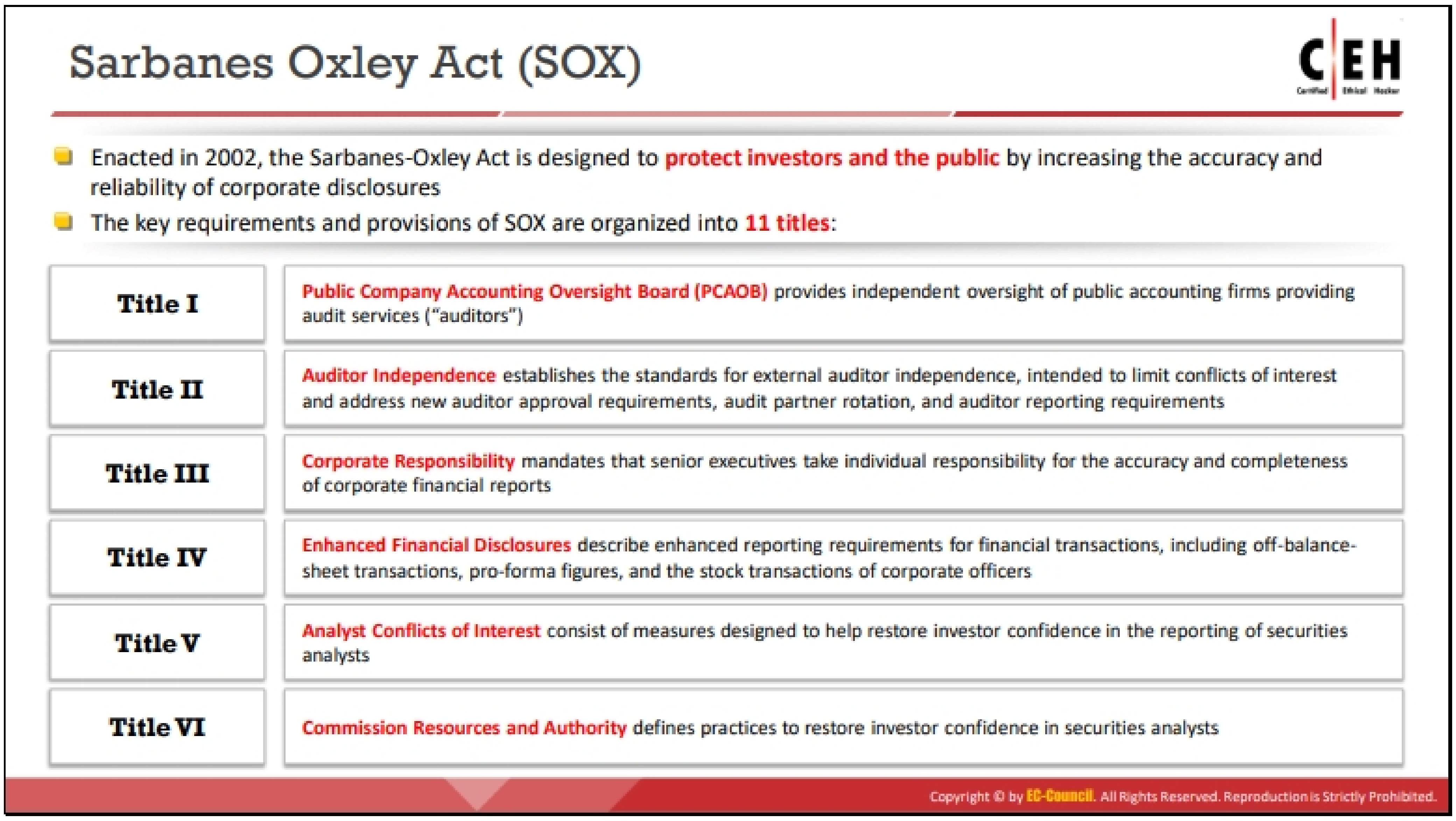
  The HIPAA requires that each employer has a standard national number that identifies them on standard transactions.

- **National Provider Identifier Standard (NPI)**

  The National Provider Identifier (NPI) is a HIPAA Administrative Simplification Standard. The NPI is a unique identification number assigned to covered health care providers. Covered health care providers and all health plans and health care clearinghouses must use the NPIs in the administrative and financial transactions adopted under HIPAA. The NPI is a 10-position, intelligence-free numeric identifier (10-digit number). This means that the numbers do not carry other information about healthcare providers, such as the state in which they live or their medical specialty.

- **Enforcement Rule**

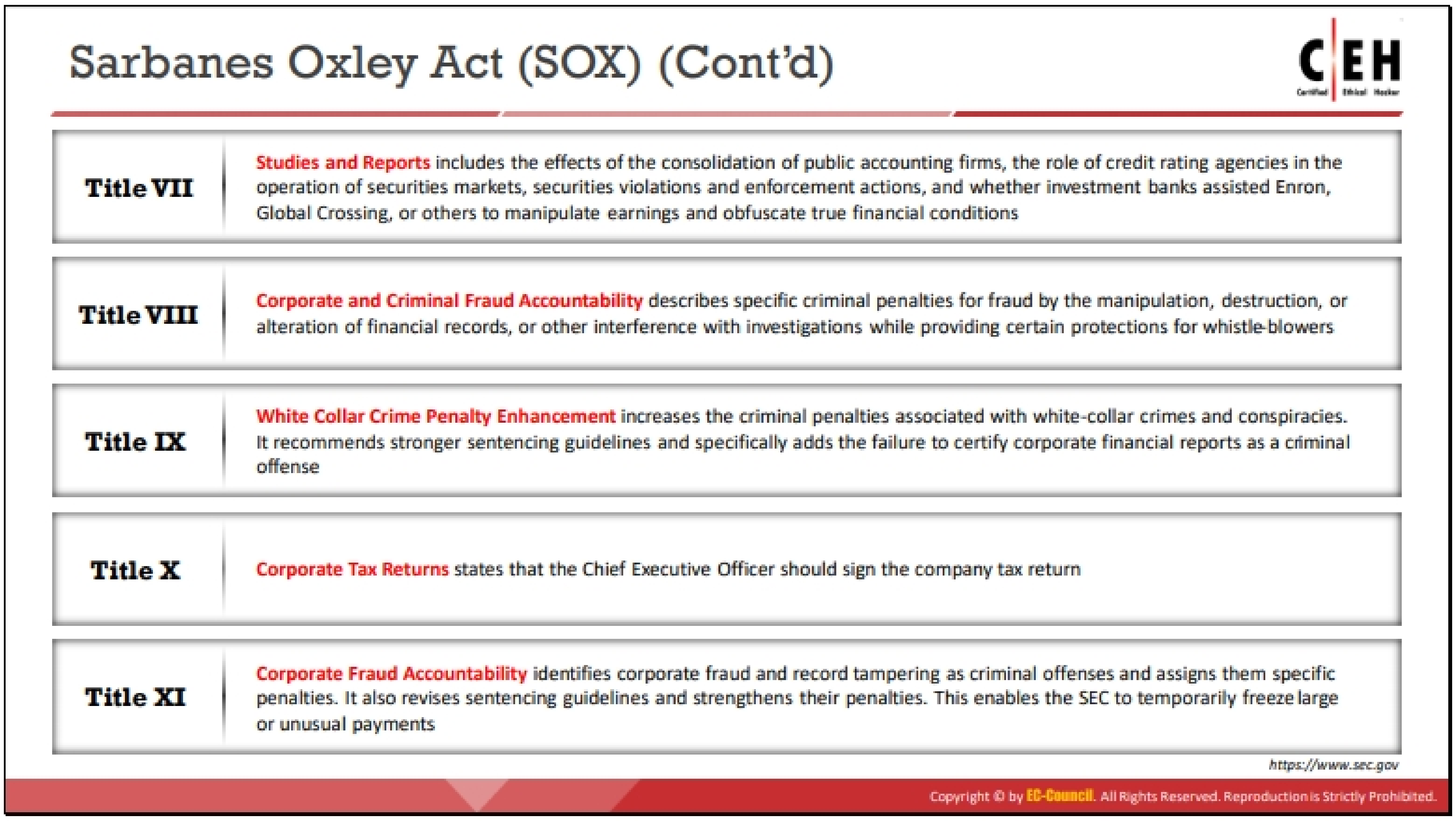
  The HIPAA Enforcement Rule contains provisions relating to compliance and investigation, as well as the imposition of civil monetary penalties for violations of the HIPAA Administrative Simplification Rules and procedures for hearings.



Sarbanes Oxley Act (SOX)

- Enacted in 2002, the Sarbanes-Oxley Act is designed to **protect investors and the public** by increasing the accuracy and reliability of corporate disclosures
- The key requirements and provisions of SOX are organized into **11 titles**:

Title I	**Public Company Accounting Oversight Board (PCAOB)** provides independent oversight of public accounting firms providing audit services ("auditors")
Title II	**Auditor Independence** establishes the standards for external auditor independence, intended to limit conflicts of interest and address new auditor approval requirements, audit partner rotation, and auditor reporting requirements
Title III	**Corporate Responsibility** mandates that senior executives take individual responsibility for the accuracy and completeness of corporate financial reports
Title IV	**Enhanced Financial Disclosures** describe enhanced reporting requirements for financial transactions, including off-balance-sheet transactions, pro-forma figures, and the stock transactions of corporate officers
Title V	**Analyst Conflicts of Interest** consist of measures designed to help restore investor confidence in the reporting of securities analysts
Title VI	**Commission Resources and Authority** defines practices to restore investor confidence in securities analysts



Sarbanes Oxley Act (SOX) (Cont'd)

Title VII	**Studies and Reports** includes the effects of the consolidation of public accounting firms, the role of credit rating agencies in the operation of securities markets, securities violations and enforcement actions, and whether investment banks assisted Enron, Global Crossing, or others to manipulate earnings and obfuscate true financial conditions
Title VIII	**Corporate and Criminal Fraud Accountability** describes specific criminal penalties for fraud by the manipulation, destruction, or alteration of financial records, or other interference with investigations while providing certain protections for whistle-blowers
Title IX	**White Collar Crime Penalty Enhancement** increases the criminal penalties associated with white-collar crimes and conspiracies. It recommends stronger sentencing guidelines and specifically adds the failure to certify corporate financial reports as a criminal offense
Title X	**Corporate Tax Returns** states that the Chief Executive Officer should sign the company tax return
Title XI	**Corporate Fraud Accountability** identifies corporate fraud and record tampering as criminal offenses and assigns them specific penalties. It also revises sentencing guidelines and strengthens their penalties. This enables the SEC to temporarily freeze large or unusual payments

https://www.sec.gov

Sarbanes Oxley Act (SOX)

Source: *https://www.sec.gov*

Enacted in 2002, the Sarbanes-Oxley Act aims to protect the public and investors by increasing the accuracy and reliability of corporate disclosures. This act does not explain how an organization must store records but describes the records that organizations must store and the duration of their storage. The Act mandated several reforms to enhance corporate responsibility, enhance financial disclosures, and combat corporate and accounting fraud.

The key requirements and provisions of SOX are organized into 11 titles:

- **Title I: Public Company Accounting Oversight Board (PCAOB)**

  Title I consists of nine sections and establishes the Public Company Accounting Oversight Board to provide independent oversight of public accounting firms that provide audit services ("auditors"). It also creates a central oversight board tasked with registering audit services, defining the specific processes and procedures for compliance audits, inspecting and policing conduct and quality control, and enforcing compliance with the specific mandates of SOX.

- **Title II: Auditor Independence**

  Title II consists of nine sections and establishes standards for external auditor independence to limit conflicts of interest. It also addresses new auditor approval requirements, audit partner rotation, and auditor reporting requirements. It restricts auditing companies from providing non-audit services (such as consulting) for the same clients.

- **Title III: Corporate Responsibility**

  Title III consists of eight sections and mandates that senior executives take individual responsibility for the accuracy and completeness of corporate financial reports. It defines the interaction between external auditors and corporate audit committees and specifies the corporate officers' responsibility for the accuracy and validity of corporate financial reports. It enumerates specific limits on the behaviors of corporate officers and describes specific forfeitures of benefits and civil penalties for non-compliance.

- **Title IV: Enhanced Financial Disclosures**

  Title IV consists of nine sections. It describes enhanced reporting requirements for financial transactions, including off-balance-sheet transactions, pro-forma figures, and the stock transactions of corporate officers. It requires internal controls to ensure the accuracy of financial reports and disclosures and mandates both audits and reports on those controls. It also requires timely reporting of material changes in financial conditions and specific enhanced reviews of corporate reports by the SEC or its agents.

- **Title V: Analyst Conflicts of Interest**

  Title V consists of only one section that discusses the measures designed to help restore investor confidence in the reporting of securities analysts. It defines the code of conduct for securities analysts and requires that they disclose any knowable conflicts of interest.

- **Title VI: Commission Resources and Authority**

  Title VI consists of four sections and defines practices to restore investor confidence in securities analysts. It also defines the SEC's authority to censure or bar securities professionals from practice and defines the conditions to bar a person from practicing as a broker, advisor, or dealer.

- **Title VII: Studies and Reports**

  Title VII consists of five sections and requires the Comptroller General and the Securities and Exchange Commission (SEC) to perform various studies and to report their findings. The required studies and reports include the effects of the consolidation of public accounting firms, the role of credit rating agencies in the operation of securities markets, securities violations, enforcement actions, and whether investment banks assisted Enron, Global Crossing, and others to manipulate earnings and obfuscate true financial conditions.

- **Title VIII: Corporate and Criminal Fraud Accountability**

  Title VIII, also known as the “Corporate and Criminal Fraud Accountability Act of 2002,” consists of seven sections. It describes specific criminal penalties for the manipulation, destruction, or alteration of financial records or interference with investigations, while also providing certain protections for whistle-blowers.

- **Title IX: White-Collar-Crime Penalty Enhancement**

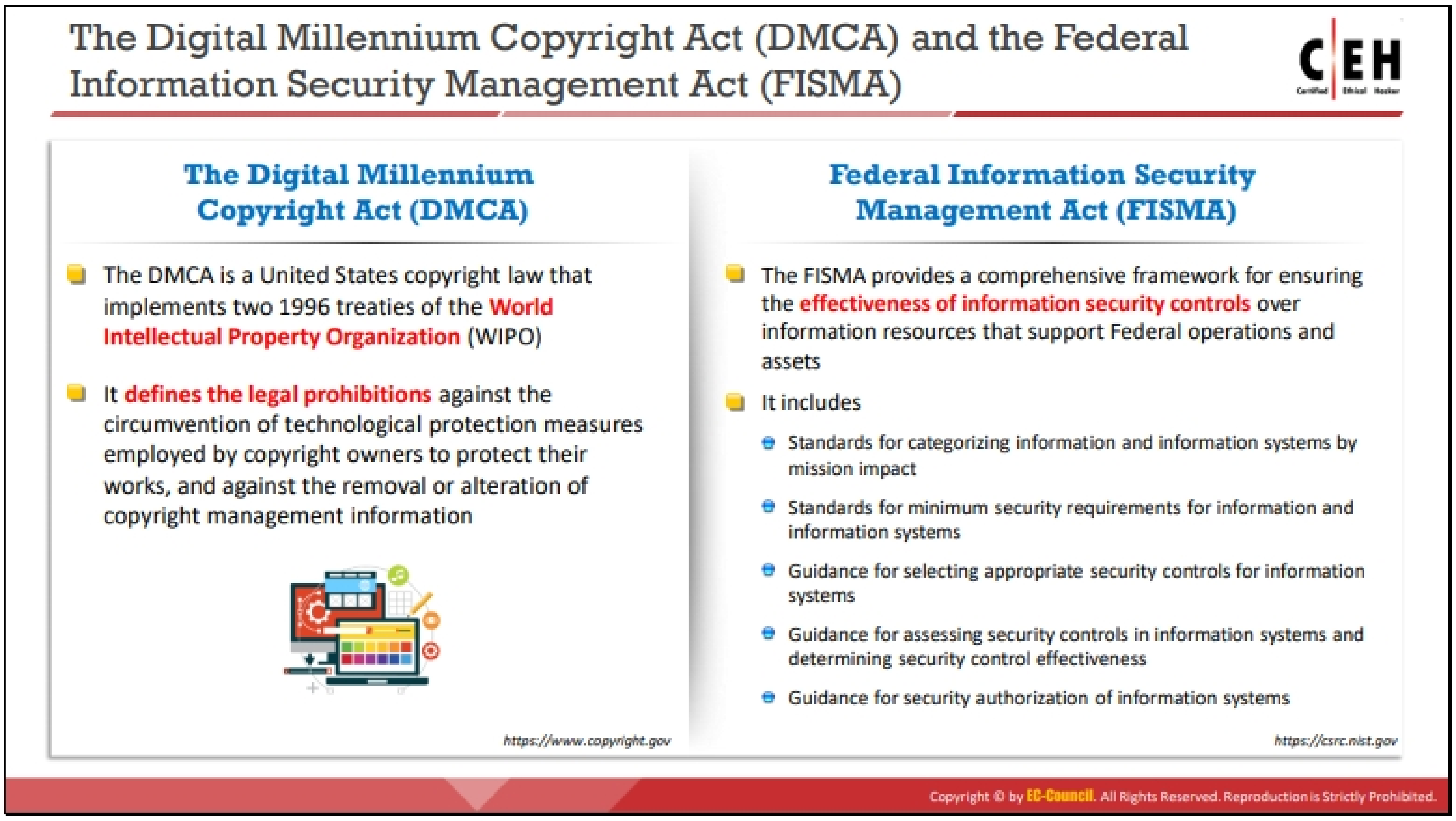
  Title IX, also known as the "White Collar Crime Penalty Enhancement Act of 2002,” consists of six sections. This title increases the criminal penalties associated with white-collar crimes and conspiracies. It recommends stronger sentencing guidelines and specifically adds failure to certify corporate financial reports as a criminal offense.

- **Title X: Corporate Tax Returns**

  Title X consists of one section that states that the Chief Executive Officer should sign the company tax return.

- **Title XI: Corporate Fraud Accountability**

  Title XI consists of seven sections. Section 1101 recommends the following name for the title: “Corporate Fraud Accountability Act of 2002.” It identifies corporate fraud and records tampering as criminal offenses and joins those offenses to specific penalties. It also revises sentencing guidelines and strengthens penalties. Doing so enables the SEC to temporarily freeze “large” or “unusual” transactions or payments.



The Digital Millennium Copyright Act (DMCA) and the Federal Information Security Management Act (FISMA)

The Digital Millennium Copyright Act (DMCA)

- The DMCA is a United States copyright law that implements two 1996 treaties of the **World Intellectual Property Organization** (WIPO)
- It **defines the legal prohibitions** against the circumvention of technological protection measures employed by copyright owners to protect their works, and against the removal or alteration of copyright management information

https://www.copyright.gov

Federal Information Security Management Act (FISMA)

- The FISMA provides a comprehensive framework for ensuring the **effectiveness of information security controls** over information resources that support Federal operations and assets
- It includes
  - Standards for categorizing information and information systems by mission impact
  - Standards for minimum security requirements for information and information systems
  - Guidance for selecting appropriate security controls for information systems
  - Guidance for assessing security controls in information systems and determining security control effectiveness
  - Guidance for security authorization of information systems

https://csrc.nist.gov

The Digital Millennium Copyright Act (DMCA)

Source: *https://www.copyright.gov*

The DMCA is an American copyright law that implements two 1996 treaties from the World Intellectual Property Organization (WIPO): the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty. In order to implement US treaty obligations, the DMCA defines legal prohibitions against circumvention of the technological protection measures employed by copyright owners to protect their works, and against the removal or alteration of copyright management information. The DMCA contains five titles:

- **Title I: WIPO TREATY IMPLEMENTATION**

  Title I implements the WIPO treaties. First, it makes certain technical amendments to US law in order to provide the appropriate references and links to the treaties. Second, it creates two new prohibitions in Title 17 of the U.S. Code—one on circumvention of the technological measures used by copyright owners to protect their works and one on tampering with copyright management information—and adds civil remedies and criminal penalties for violating the prohibitions.

- **Title II: ONLINE COPYRIGHT INFRINGEMENT LIABILITY LIMITATION**

  Title II of the DMCA adds a new section 512 to the Copyright Act to create four new limitations on liability for copyright infringement by online service providers. A service provider bases these limitations on the following four categories of conduct:

  - Transitory communications
  - System caching
  - The user-directed storage of information on systems or networks

  - Information location tools

  New section 512 also includes special rules concerning the application of these limitations to nonprofit educational institutions.

- **Title III: COMPUTER MAINTENANCE OR REPAIR**

  Title III of the DMCA allows the owner of a copy of a program to make reproductions or adaptations when necessary to use the program in conjunction with a computer. The amendment permits the owner or lessee of a computer to make or to authorize the making of a copy of a computer program in the course of maintaining or repairing that computer.

- **Title IV: MISCELLANEOUS PROVISIONS**

  Title IV contains six miscellaneous provisions. The first provision announces the Clarification of the Authority of the Copyright Office; the second grants exemption for the making of "ephemeral recordings"; the third promotes study by distance education; the fourth provides an exemption for Nonprofit Libraries and Archives; the fifth allows Webcasting Amendments to the Digital Performance Right in Sound Recordings, and, finally, the sixth provision addresses concerns about the ability of writers, directors and screen actors to obtain residual payments for the exploitation of motion pictures in situations where the producer is no longer able to make these payments.

- **Title V: PROTECTION OF CERTAIN ORIGINAL DESIGNS**

  Title V of the DMCA, entitles the Vessel Hull Design Protection Act (VHDPA). This act creates a new system for protecting the original designs of certain useful articles that make the article attractive or distinctive in appearance. For purposes of the VHDPA, "useful articles" are limited to the hulls (including the decks) of vessels no longer than 200 feet.

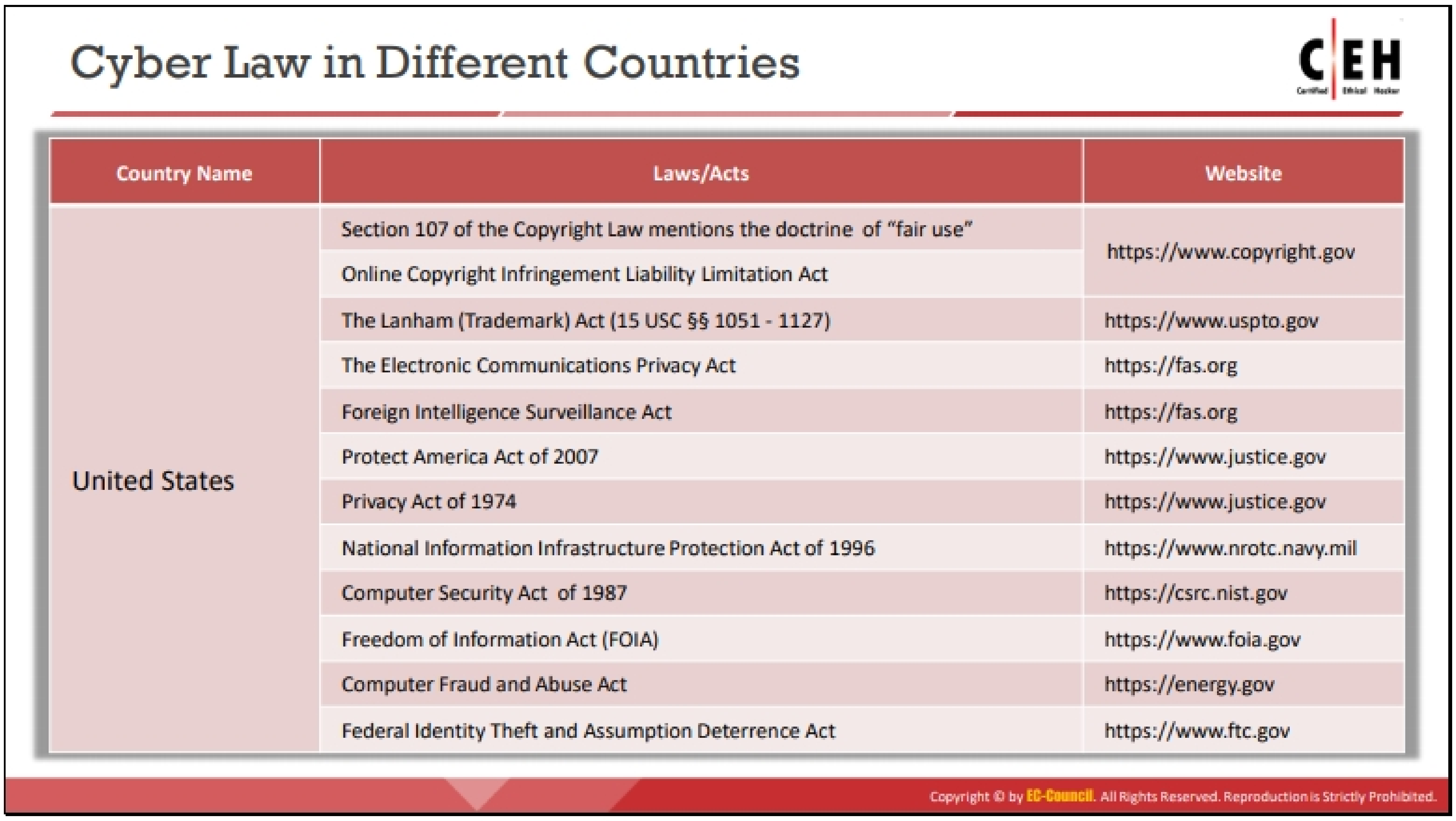
The Federal Information Security Management Act (FISMA)

Source: *https://csrc.nist.gov*

The Federal Information Security Management Act of 2002 was enacted to produce several key security standards and guidelines required by Congressional legislation. The FISMA provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. It requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or another source. The FISMA framework includes:

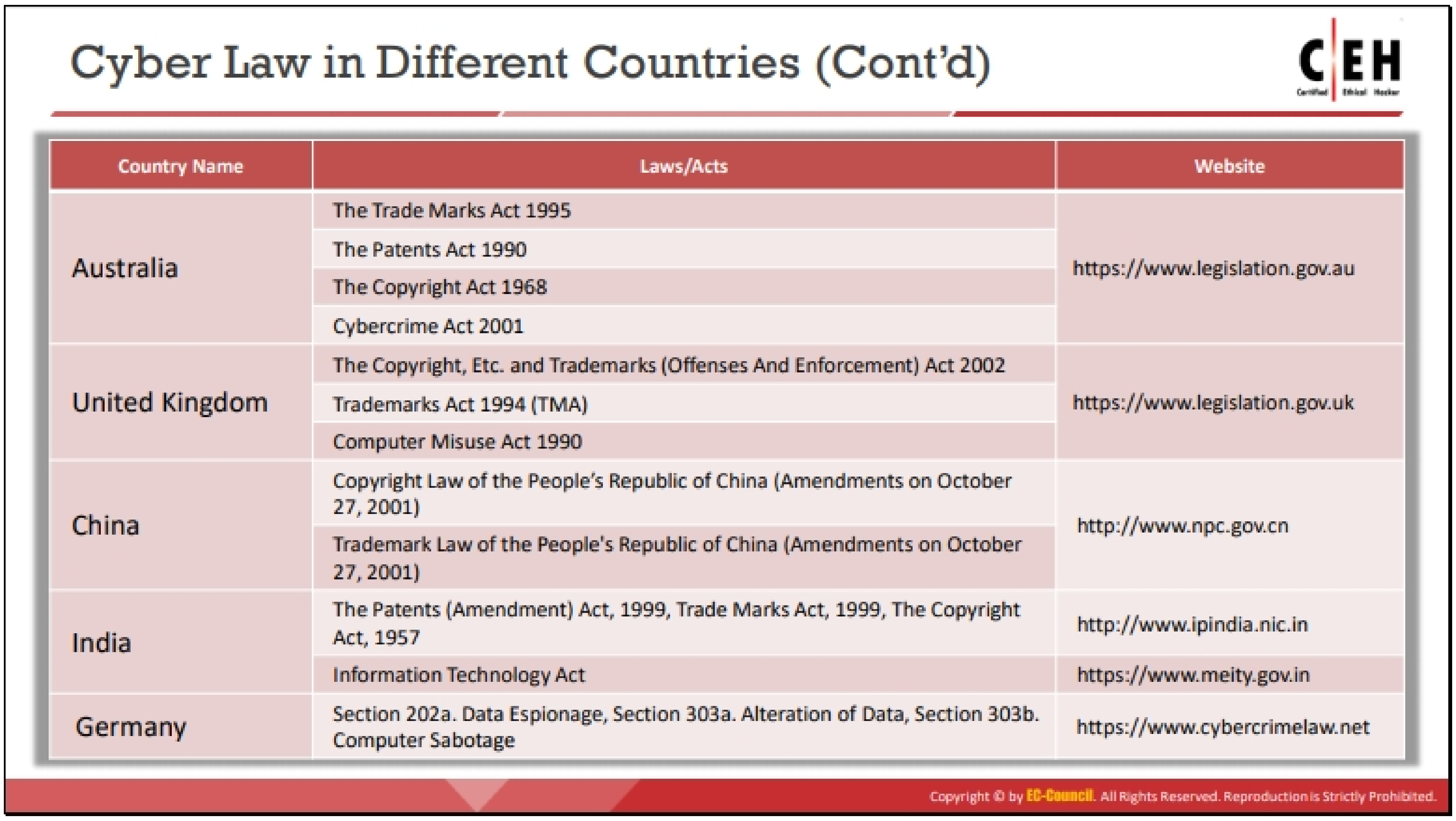
- Standards for categorizing information and information systems by mission impact
- Standards for the minimum security requirements for information and information systems
- Guidance for selecting appropriate security controls for information systems

- Guidance for assessing security controls in information systems and determining their effectiveness
- Guidance for the security authorization of information systems



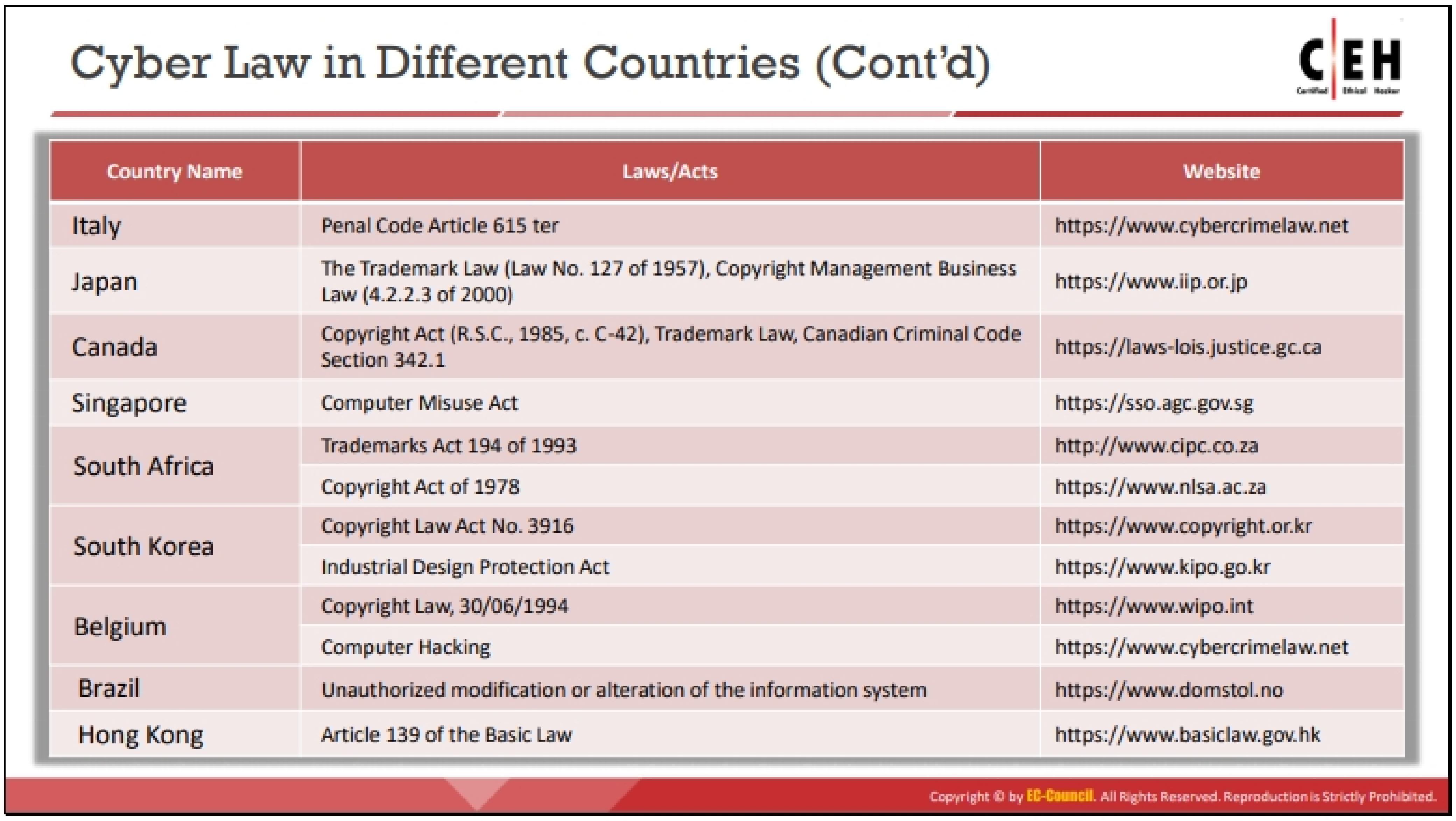
Cyber Law in Different Countries

Country Name	Laws/Acts	Website
United States	Section 107 of the Copyright Law mentions the doctrine of "fair use"	https://www.copyright.gov
	Online Copyright Infringement Liability Limitation Act	
	The Lanham (Trademark) Act (15 USC §§ 1051 - 1127)	https://www.uspto.gov
	The Electronic Communications Privacy Act	https://fas.org
	Foreign Intelligence Surveillance Act	https://fas.org
	Protect America Act of 2007	https://www.justice.gov
	Privacy Act of 1974	https://www.justice.gov
	National Information Infrastructure Protection Act of 1996	https://www.nrotc.navy.mil
	Computer Security Act of 1987	https://csrc.nist.gov
	Freedom of Information Act (FOIA)	https://www.foia.gov
	Computer Fraud and Abuse Act	https://energy.gov
	Federal Identity Theft and Assumption Deterrence Act	https://www.ftc.gov



Cyber Law in Different Countries (Cont'd)

Country Name	Laws/Acts	Website
Australia	The Trade Marks Act 1995	https://www.legislation.gov.au
	The Patents Act 1990	
	The Copyright Act 1968	
	Cybercrime Act 2001	
United Kingdom	The Copyright, Etc. and Trademarks (Offenses And Enforcement) Act 2002	https://www.legislation.gov.uk
	Trademarks Act 1994 (TMA)	
	Computer Misuse Act 1990	
China	Copyright Law of the People's Republic of China (Amendments on October 27, 2001)	http://www.npc.gov.cn
	Trademark Law of the People's Republic of China (Amendments on October 27, 2001)	
India	The Patents (Amendment) Act, 1999, Trade Marks Act, 1999, The Copyright Act, 1957	http://www.ipindia.nic.in
	Information Technology Act	https://www.meity.gov.in
Germany	Section 202a. Data Espionage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage	https://www.cybercrimelaw.net



Cyber Law in Different Countries (Cont'd)

Country Name	Laws/Acts	Website
Italy	Penal Code Article 615 ter	https://www.cybercrimelaw.net
Japan	The Trademark Law (Law No. 127 of 1957), Copyright Management Business Law (4.2.2.3 of 2000)	https://www.iip.or.jp
Canada	Copyright Act (R.S.C., 1985, c. C-42), Trademark Law, Canadian Criminal Code Section 342.1	https://laws-lois.justice.gc.ca
Singapore	Computer Misuse Act	https://sso.agc.gov.sg
South Africa	Trademarks Act 194 of 1993	http://www.cipc.co.za
	Copyright Act of 1978	https://www.nlsa.ac.za
South Korea	Copyright Law Act No. 3916	https://www.copyright.or.kr
	Industrial Design Protection Act	https://www.kipo.go.kr
Belgium	Copyright Law, 30/06/1994	https://www.wipo.int
	Computer Hacking	https://www.cybercrimelaw.net
Brazil	Unauthorized modification or alteration of the information system	https://www.domstol.no
Hong Kong	Article 139 of the Basic Law	https://www.basiclaw.gov.hk

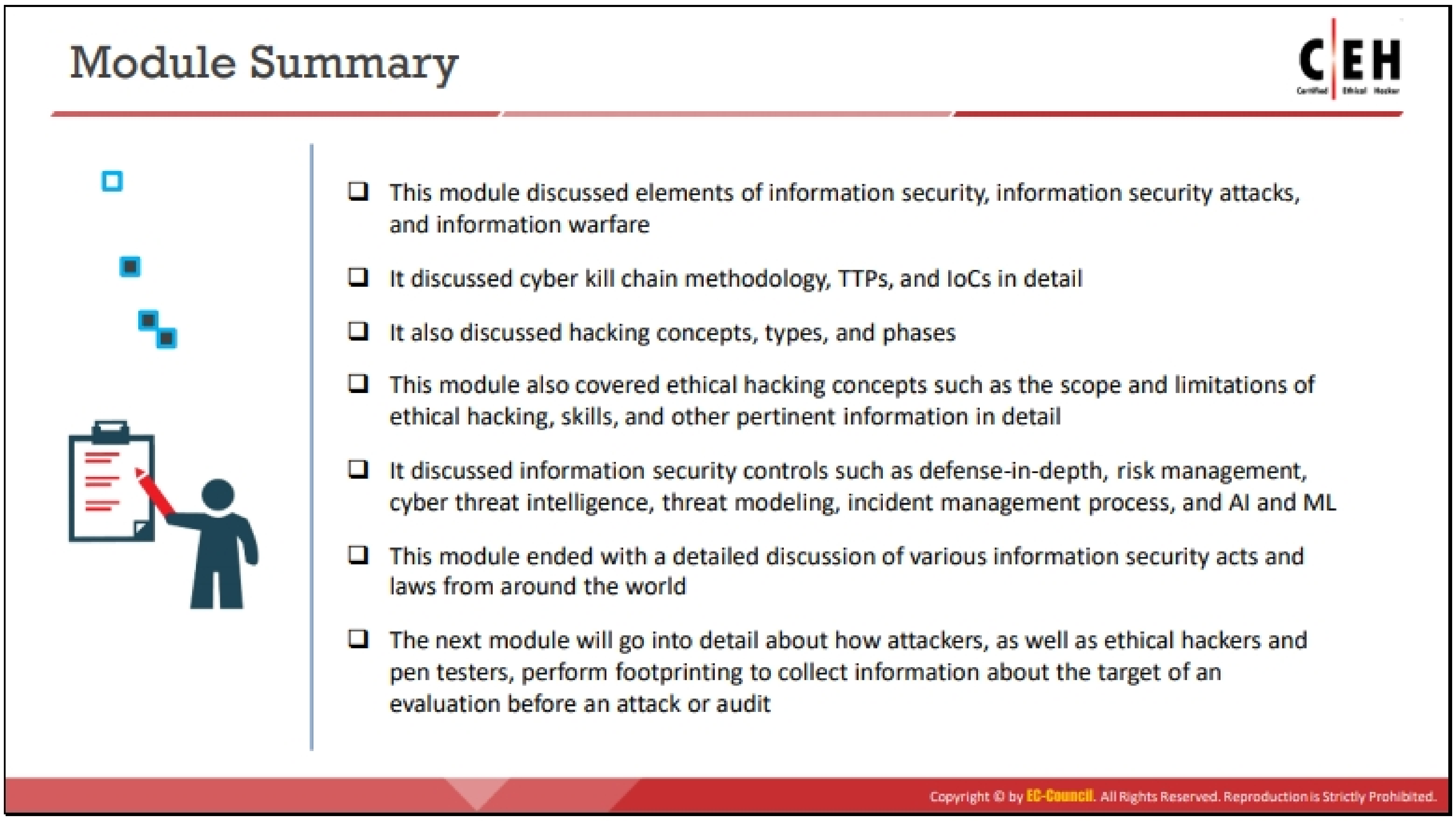
Cyber Law in Different Countries

Cyberlaw or Internet law refers to any laws that deal with protecting the Internet and other online communication technologies. Cyberlaw covers topics such as Internet access and usage, privacy, freedom of expression, and jurisdiction. Cyber laws provide an assurance of the integrity, security, privacy, and confidentiality of information in both governmental and private organizations. These laws have become prominent due to the increase in Internet usage around the world. Cyber laws vary by jurisdiction and country, so implementing them is quite challenging. Violating these laws results in punishments ranging from fines to imprisonment.

Country Name	Laws/Acts	Website
United States	Section 107 of the Copyright Law mentions the doctrine of "fair use"	https://www.copyright.gov
	Online Copyright Infringement Liability Limitation Act	
	The Lanham (Trademark) Act (15 USC §§ 1051 - 1127)	https://www.uspto.gov
	The Electronic Communications Privacy Act	https://fas.org
	Foreign Intelligence Surveillance Act	https://fas.org
	Protect America Act of 2007	https://www.justice.gov
	Privacy Act of 1974	https://www.justice.gov
	National Information Infrastructure Protection Act of 1996	https://www.nrotc.navy.mil
	Computer Security Act of 1987	https://csrc.nist.gov
	Freedom of Information Act (FOIA)	https://www.foia.gov

	Computer Fraud and Abuse Act	https://energy.gov
	Federal Identity Theft and Assumption Deterrence Act	https://www.ftc.gov
Australia	The Trade Marks Act 1995	https://www.legislation.gov.au
	The Patents Act 1990	
	The Copyright Act 1968	
	Cybercrime Act 2001	
United Kingdom	The Copyright, Etc. and Trademarks (Offenses And Enforcement) Act 2002	https://www.legislation.gov.uk
	Trademarks Act 1994 (TMA)	
	Computer Misuse Act 1990	
China	Copyright Law of the People's Republic of China (Amendments on October 27, 2001)	http://www.npc.gov.cn
	Trademark Law of the People's Republic of China (Amendments on October 27, 2001)	
India	The Patents (Amendment) Act, 1999, Trade Marks Act, 1999, The Copyright Act, 1957	http://www.ipindia.nic.in
	Information Technology Act	https://www.meity.gov.in
Germany	Section 202a. Data Espionage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage	https://www.cybercrimelaw.net
Italy	Penal Code Article 615 ter	https://www.cybercrimelaw.net
Japan	The Trademark Law (Law No. 127 of 1957), Copyright Management Business Law (4.2.2.3 of 2000)	https://www.iip.or.jp
Canada	Copyright Act (R.S.C., 1985, c. C-42), Trademark Law, Canadian Criminal Code Section 342.1	https://laws-lois.justice.gc.ca
Singapore	Computer Misuse Act	https://sso.agc.gov.sg
South Africa	Trademarks Act 194 of 1993	http://www.cipc.co.za
	Copyright Act of 1978	https://www.nlsa.ac.za
South Korea	Copyright Law Act No. 3916	https://www.copyright.or.kr
	Industrial Design Protection Act	https://www.kipo.go.kr
Belgium	Copyright Law, 30/06/1994	https://www.wipo.int
	Computer Hacking	https://www.cybercrimelaw.net
Brazil	Unauthorized modification or alteration of the information system	https://www.domstol.no
Hong Kong	Article 139 of the Basic Law	https://www.basiclaw.gov.hk

Table 1.4: Cyber Law in Different Countries



Module Summary

☐ This module discussed elements of information security, information security attacks, and information warfare

☐ It discussed cyber kill chain methodology, TTPs, and IoCs in detail

☐ It also discussed hacking concepts, types, and phases

☐ This module also covered ethical hacking concepts such as the scope and limitations of ethical hacking, skills, and other pertinent information in detail

☐ It discussed information security controls such as defense-in-depth, risk management, cyber threat intelligence, threat modeling, incident management process, and AI and ML

☐ This module ended with a detailed discussion of various information security acts and laws from around the world

☐ The next module will go into detail about how attackers, as well as ethical hackers and pen testers, perform footprinting to collect information about the target of an evaluation before an attack or audit

Module Summary

This module has discussed elements of information security, information security attacks, and information warfare. It has covered cyber kill chain methodology, TTPs, and IoCs in detail. It also discussed hacking concepts, types, and phases. This module closely examined ethical hacking concepts such as its scope and limitations and the skills of an ethical hacker. It also covered the topic of information security controls such as defense-in-depth, risk management, cyber threat intelligence, threat modeling, incident management process, and AI and ML. Finally, this module ended with a detailed discussion of various information security acts and laws.

The next module will examine how attackers, as well as ethical hackers and pen testers, perform footprinting to collect information about their target before an attack or audit.